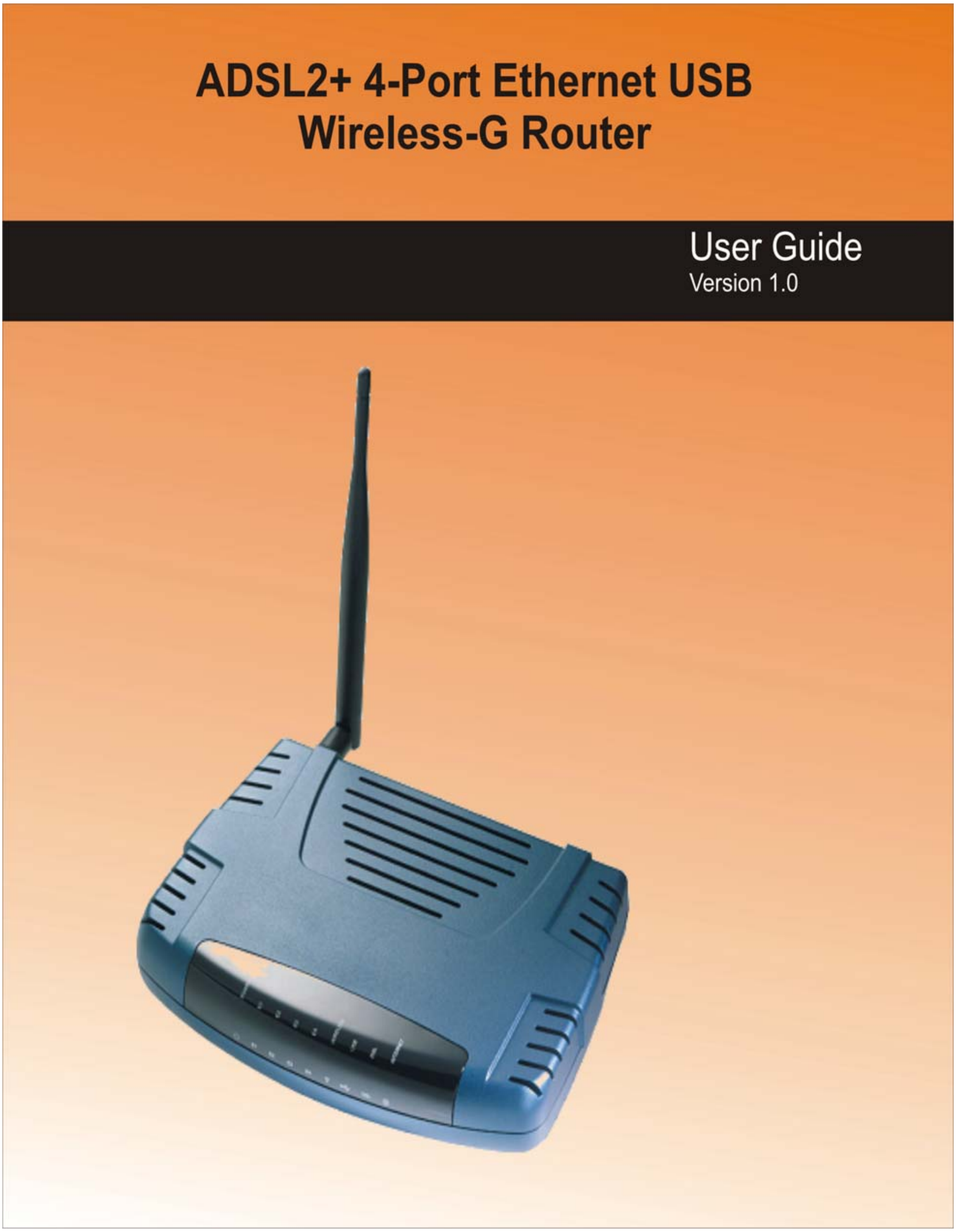


ADSL2+ 4-Port Ethernet USB Wireless-G Router

User Guide

Version 1.0

Table of Contents

Preliminary Pages **Page**

Table of Contents 2

List of Ilustrations..5

Chapter 1 - About this Manual 11

1.1 Introduction 11

1.2 Scope and Purpose..11

1.3 Targeted Audience..11

1.4 Manual Organization..11

Chapter 2 – ADSL Router Description...12

2.1 ADSL Router Overview...12

Chapter 3 - Your Gateway At A Glance..13

3.1 Ports and Buttons..13

3.2 ADSL Router Overview...14

3.2.1 Front Indicators 14

3.2.2 Back Panel..15

Chapter 4 - Setting Up the ADSL Router..16

4.1 Logging into your ADSL Router..16

4.2 Quick Start..18

4.3 LAN / DHCP Configuration...18

4.4 Diagnostic Test...20

4.4.1 Ping Test...21

4.4.2 Modem Test..21

4.5 Advanced..22

4.5.1 WAN Connection...22

4.5.2 New Connection...23

4.5.3 ADSL Modulation..24

4.5.4 Connection Scan...25

4.5.5 VCC List...25

4.5.6 Quickstart 26

4.5.7 LAN Configuration 28

4.5.8 LAN Clients 29

4.5.9 Ethernet Switch Configuration...30

4.5.10 Application (UPnP) 31

4.5.11 SNTP 32
4.5.12 SNMP 33
4.5.13 IGMP Proxy 34
4.5.14 TR-068 WAN Access..36
4.5.15 TR-069..37
4.5.16 NAT Services 38
4.5.17 DNS Proxy 39
4.5.18 Dynamic DNS Client..40
4.5.19 Easy Connect Configuration...41
4.5.20 Port Triggering 42
4.5.21 Port Forwarding...42
4.5.22 Bridge Filters 44
4.5.23 Web Access Control...45
4.5.23.1 Enable Web Access Control (WAN-Side) 45
4.5.24 SSH Access Control 46
4.5.24.1 Enable SSH Access Control (WAN-Side) 46
4.5.25 QoS...47
4.5.26 Egress 48
4.5.26.1 No Egress Mode 48
4.5.26.2 Egress Layer 2 Configuration.......................................49
4.5.26.3 Egress Layer 3 Configuration.......................................50
4.5.27 Ingress 51
4.5.27.1 Ingress Untrusted Mode 51
4.5.27.2 Ingress Layer 2 Configuration......................................52
4.5.27.3 Ingress Layer 3 Configuration......................................54
4.5.27.4 Ingress Static Configuration...56
4.5.28 QoS Shaper Configuration 57
4.5.29 Policy Routing Configuration 61
4.5.30 Static Routing 64
4.5.31 Dynamic Routing...65
4.5.32 Routing Table 66
4.5.33 System Password..66
4.5.34 Firmware Upgrade...67
4.5.35 Restore to Default..67
4.6 Wireless 68
4.6.1 Wireless Setup 68

4.6.2 Wireless Configuration....69
4.6.3 Multiple SSID....70
4.6.4 Wireless Security....71
4.6.4.1 WEP....71
4.6.4.2 802.1x....72
4.6.4.3 WPA....73
4.6.5 Wireless Management....74
4.6.5.1 Access List....74
4.6.5.2 Associated Stations....74
4.6.6 WDS....75
4.7 Security....77
4.7.1 IP Filters....77
4.7.2 LAN Isolation....78
4.7.3 URL Filters....78
4.8 Status....79
4.8.1 Connection Status....80
4.8.2 System Log....80
4.8.3 Remote Log Settings....81
4.8.4 Network Statistics....82
4.8.5 DDNS Update Status....82
4.8.6 DHCP Clients....83
4.8.7 QoS Status....84
4.8.8 Modem Status....84
4.8.9 Product Information....85
4.8.10 WDS Report....86
4.9 Help....87

List of Ilustrations

Figure **Page**

Figure 1-1 : Wireless-G System Configuration Diagram..12

Figure 1-2 : Front Indicators 14

Figure 1-3 : Back Panel Indicators...15

Figure 1-4 : Setup Page 16

Figure 1-5 : Internet Login Account Setting 17

Figure 1-6 : Basic Home 17

Figure 1-7 : Quick Start Page...18

Figure 1-8 : LAN / DHCP Configuration..19

Figure 1-9 : Diagnostics Test Screen 20

Figure 1-10 : Diagnostics Test Result Screen 20

Figure 1-11 : Ping Test Screen...21

Figure 1-12 : Modem Test...21

Figure 1-13 : Advanced Screen..22

Figure 1-14 : New Connection (PPPoE Connection Setup)...................................23

Figure 1-15 : ADSL Modulation (Modem Setup)...24

Figure 1-16 : Connection Scan...25

Figure 1-17 : VCC List...25

Figure 1-18 : Quickstart (PPPoE Connection Setup) 27

Figure 1-19 : LAN Configuration 28

Figure 1-20 : LAN Clients 29

Figure 1-21 : Ethernet Switch Configuration..30

Figure 1-22 : UPnP...31

Figure 1-23 : SNTP 32

Figure 1-24 : SNMP Management 33

Figure 1-25 : IGMP Proxy 34

Figure 1-26 : TR-068 WAN Access..36

Figure 1-27 : TR-069..37

Figure 1-28 : NAT Services 38

Figure 1-29 : DNS Proxy 39

Figure 1-30 : Dynamic DNS Client...40

Figure 1-31 : Easy Connect Configuration 41

Figure 1-32 : Port Triggering 42

Figure 1-33 : Port Forwarding...43

Figure 1-34 : MAC Filtering (Bridge Filters) 44

Figure 1-35 : Web Access Control..45

Figure 1-36 : SSH Access Control 46

Figure 1-37 : No Egress 48

Figure 1-38 : Egress Layer 2 49

Figure 1-39 : Egress Layer 3 50

Figure 1-40 : Ingress Untrusted Mode 51

Figure 1-41 : Ingress Layer 2 Configuration..52

Figure 1-42 : Ingress Layer 3 Configuration..54

Figure 1-43 : Ingress Static Configuration...56

Figure 1-44 : QoS Shaper Configuration 57

Figure 1-45 : HTB Queue Discipline enabled...58

Figure 1-46 : Low Latency Queue Discipline enabled 59

Figure 1-47 : PRIOWRR enabled 60

Figure 1-48 : Policy Routing Configuration 61

Figure 1-49 : Static Routing...64

Figure 1-50 : Dynamic Routing 65

Figure 1-51 : Routing Table...66

Figure 1-52 : System Password...66

Figure 1-53 : Firmware Upgrade..67

Figure 1-54 : Restore to Default prompt 67

Figure 1-55 : Wireless Setup Page 68

Figure 1-56 : Wireless Configuration Page 69

Figure 1-57 : Multiple SSID 70

Figure 1-58 : Wireless Security 71

Figure 1-59 : Wireless Security – WEP 72

Figure 1-60 : Wireless Security – 802.1x 72

Figure 1-61 : Wireless Security - WPA 73

Figure 1-62 : Wireless Management 74

Figure 1-63 : WDS 75

Figure 1-64 : Security 77

Figure 1-65 : IP Filters 77

Figure 1-66 : LAN Isolation 78

Figure 1-67 : URL Filters 78

Figure 1-68 : Status 79

Figure 1-69 : Connection Status 80

Figure 1-70 : System Log 80

Figure 1-71 : Remote Log Settings 81

Figure 1-72 : Network Statistics 82

Figure 1-73 : DDNS Update Status 82

Figure 1-74 : DDNS Status (DDNS Client Enabled) 83

Figure 1-75 : DHCP Clients 83

Figure 1-76 : QoS Status 84

Figure 1-77 : Modem Status 84

Figure 1-78 : Product Information 85

Figure 1-79 : WDS Report 86

Figure 1-80 : Help Screen 87

Declaration Of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

Countries of Operation and Conditions of Use in the European Community

This device is intend to be operated in all countries of the European Community. Requirement is for indoors vs. outdoors operation, license requirements and allowed channels of operation apply in some countries as described in this document.

> Note… ⚠
> The user must use the configuration utility provided with this product to check the current channel of operation and confirm that the devices operating in conformance with the spectrum usage rules for the European Community countries as described below.

If operation is occurring outside of the allowable channels as indicated in this guide, then the user must cease operating the product and consult with the local technical support staff responsible for the wireless network.

This device may be operated **indoors or outdoors** in all countries of the European Community using the 2.4GHz band: **Channels 1 – 13**, except where noted below:

- In **Italy** the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In **France** outdoor operation is only permitted using the 2.4 – 2.454 GHz band: Channels 1 – 7.

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by the party responsible, could void the user’s right to operate the equipment.

RF Exposure

This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PCMCIA slots, which can provide 1 cm separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operate in conjunction with another antenna or transmitter.

Safety Summary Messages

WARNING
HIGH VOLTAGE

is used in the equipment. Make sure equipment is properly grounded BEFORE opening. Failure to observe safety precautions may result in electric shock to user.

CAUTION

Check voltages before connecting equipment to power supplies. Wrong voltages applied may result in damage to equipment.

Chapter 1 - About this Manual

1.1 Introduction

This manual provides a general product overview and description of its subsystems and components and basic operation and preventive maintenance instructions of the ADSL2+ 4 port Ethernet USB Wireless Router.

1.2 Scope and Purpose

This manual provides the following:

- An overview of the Wireless-G system configuration and connectivity;
- General description and specifications of the Wireless-G system components;
- Operating instructions of the system and equipment;

1.3 Targeted Audience

This manual is designed and developed for the operators and users who are required to operate and perform first-level maintenance of the ADSL2+ 4 Port Ethernet USB Wireless Router. It assumes the user of this manual has basic knowledge and experience in operating similar modem configuration and computer systems equipment.

1.4 Manual Organization

The manual is divided into the following chapters:

1. ***Chapter 1** – About this Manual;* this chapter provides an introduction to the manual’s scope and purpose, targeted audience and contents organisation.
2. ***Chapter 2** – ADSL Router Description;* this chapter provides the system description and system configuration diagram of ADSL Router connection.
3. ***Chapter 3** – Your Gateway At A Glance;* this chapter provides an overview of ports and LEDs, Front and Back indicators of the 4-Port Ethernet ADSL Router.
4. ***Chapter 4 –** Setting Up the ADSL Router;* this chapter provides description of all function within the Web User Interface.

Chapter 2 – ADSL Router Description

The ADSL2+ 4 port Ethernet USB Wireless Router is a high-speed WAN bridge/router. This full-featured product is specifically designed to allow maximum of 4 Ethernet-workstations to be connected to the Internet and directly connect to your local area network via high speed 10/100 Mbps Ethernet. Users using wireless workstations will be able to connect to the Internet using 802.11g wireless technology. The ADSL Router has also full NAT firewall and DMZ services to block unwanted users from accessing your network.

For game users, the ADSL Router had already pre configured for several low latency game ports. Just click on the game you are playing on line and the rest is done for you.

The ADSL Router is fully compatible with all PCs; as long as the PC supports an Ethernet interface and is running a TCP/IP protocol stack, your PC can have high-speed WAN access. So, plug in the ADSL Router (refer to easy start guide), configure it (per your ISP's requirements) and enjoy the fast Internet access like never before.

2.1 ADSL Router Overview

Figure 1-1 shows the system configuration diagram of a typical Wireless-G router connection.

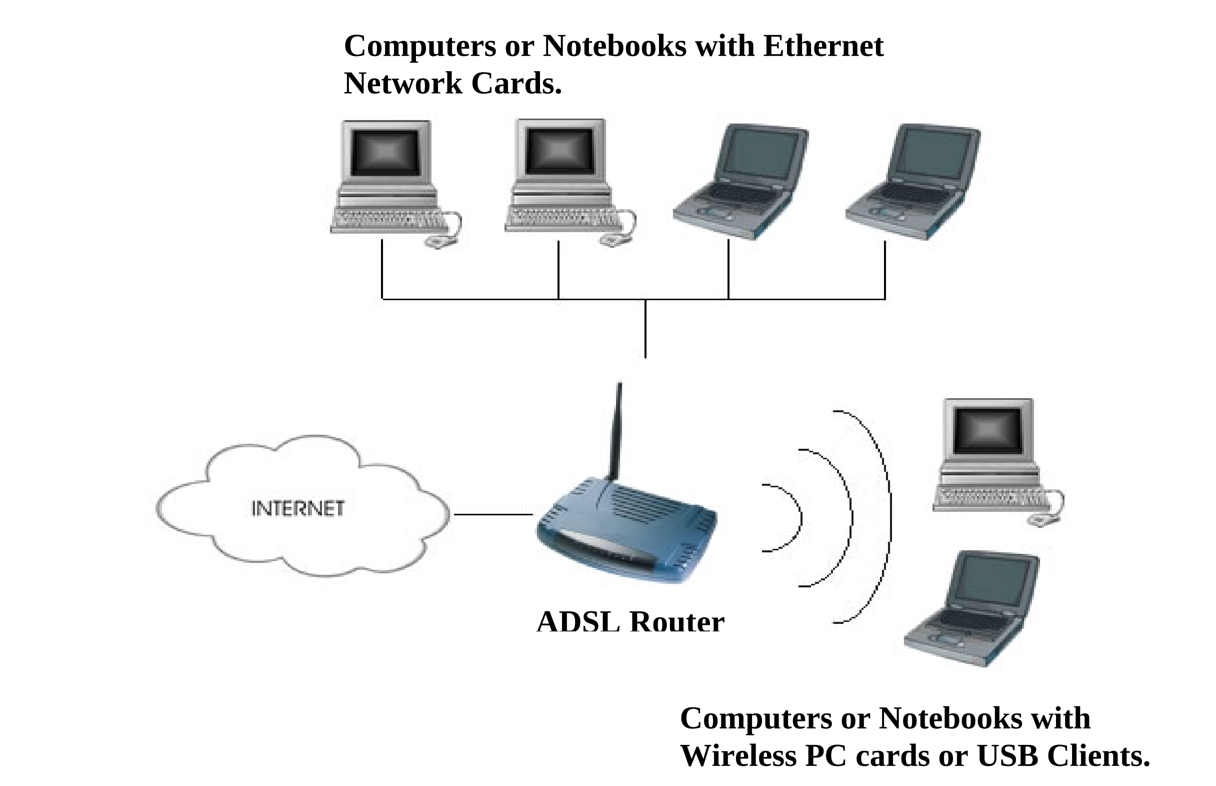

Computers or Notebooks with Ethernet Network Cards.
INTERNET
ADSL Router
Computers or Notebooks with Wireless PC cards or USB Clients.

Figure 1-1 : Wireless-G System Configuration Diagram

Chapter 3 - Your Gateway At A Glance

The ADSL Wireless LAN 802.11g 4 Port Ethernet & USB Combo 4 Port Router may have different ports and LEDs. Let’s take a look at the different options. Depending on your model, it may have some or all of the features listed below.

3.1 Ports and Buttons

Reset and Restore to Factory Defaults: The restore to factory defaults feature will set the ADSL Router to its factory default configuration by resetting the ADSL Router. You may need to place the ADSL Router into its factory defaults if the configuration is changed; you lose the ability to interface to the ADSL Router via the web interface, or following a software upgrade. To reset the ADSL Router, simply press the reset button for about approximately 10 seconds. The ADSL Router will be reset to its factory defaults and after about 30 ~ 40 seconds the ADSL Router will become operational again.

LAN (local area network) E1 to E4 port(s): connects to Ethernet network devices, such as a PC, hub, switch, or routers. The ports are 10/100 Base-T Auto-MDI/MDIX (allows either cross or straight cable) Ethernet jack (RJ-45) to connect to your Ethernet Network card or Ethernet Hub / Switch.

Power: This is where you connect the power. Make sure to observe the proper power requirements. The required power is 9 volts.

USB (universal serial port): connects to a PC’s USB port. The ADSL Router only supports Window’s based PCs via an RNDIS driver (included in the software).

DSL port: This is the WAN interface that connects directly to your phone line.

3.2 ADSL Router Overview

3.2.1 Front Indicators

Figure 1-2 shows the front indicators of the Wireless-G router.

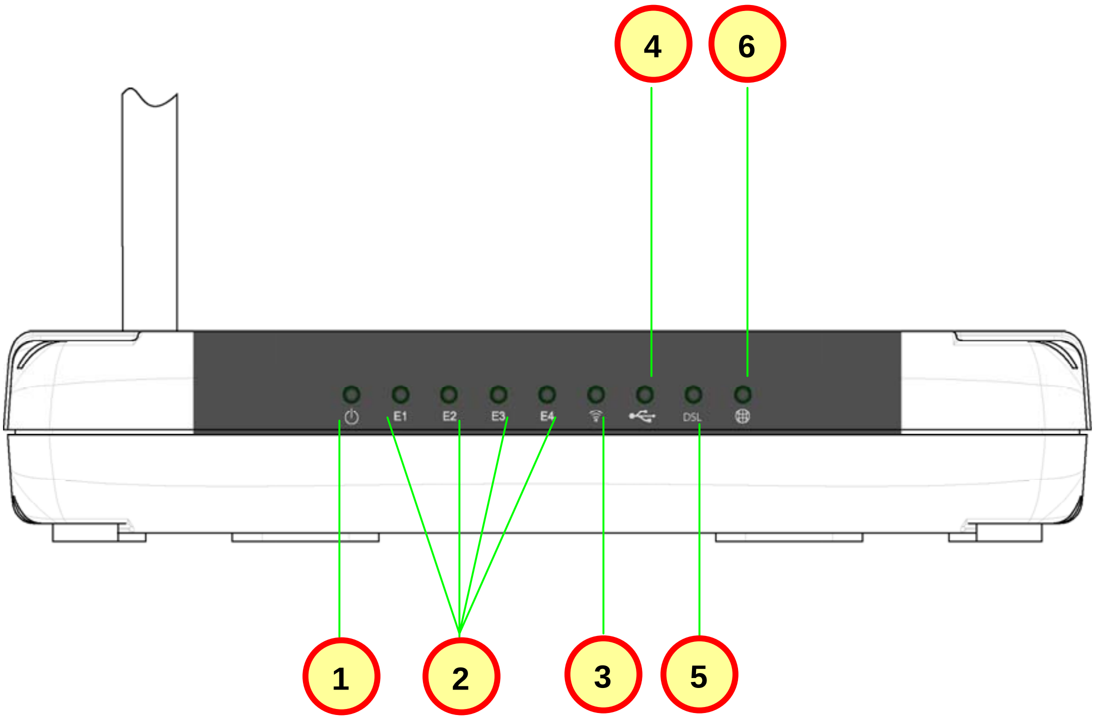


Figure 1-2 : Front Indicators

LED Name	Status & Meaning
1. **Power**	**Lights up** when power is supplied to the ADSL Router.
2. **Ethernet(E1 - E4)**	**Lights up** when the Ethernet cable is properly connected from your ADSL Router to the Ethernet Card. **Flickers** when the ADSL is transmitting/receiving data.
3. **Wireless**	**Flickers** when the Wireless LAN is operational.
4. **USB**	**Lights up** when the USB cable is properly connected from your ADSL Router to the USB slot. **Lights Off** when the USB cable is not connected or it is properly disconnected.
5. **DSL**	**Lights off** when no Telephone jack (RJ-11) is connected. **Flickers** when the ADSL Router is trying to establish a connection with the ADSL Service Provider (Training). Steady Green LED. **Lights up** when the ADSL connection is established.
6. **Internet**	Green LED **lights up** when the PPP connection is established. **Lights off** when no PPP connection.

3.2.2 Back Panel

Figure 1-3 shows the back panel indicators of the Wireless-G router.

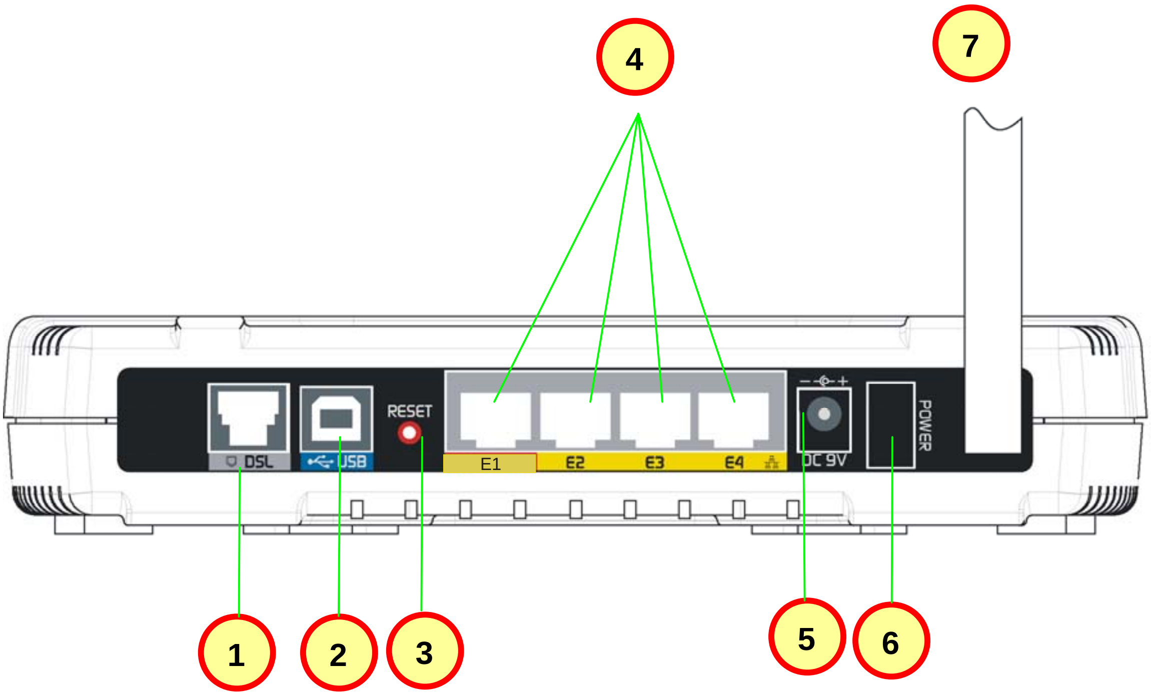


Figure 1-3 : Back Panel Indicators

Label	Description
1. **DSL**	Connect the telephone jack (RJ-11) to your Telephone Wall Socket (DSL line).
2. **USB**	Connect the USB jack to your PC's USB slot.
3. **RESET**	To reset the ADSL Router, simply press the reset button for about 10 seconds (all customised settings that you have saved will be lost!).
4. **ETHERNET(E1-E4)**	10/100 Base-T Auto-MDI/MDIX Ethernet jack (RJ-45) to connect to your PC's Ethernet Network card or Ethernet Hub / Switch.
5. **DC 9V**	To connect to the Power Adapter that comes with your package.
6. **POWER SWITCH**	Push downwards to switch ON and lift upwards to switch OFF.
7. **RF Antenna**	180° 2.4Ghz Wireless Antenna.

Chapter 4 - Setting Up the ADSL Router

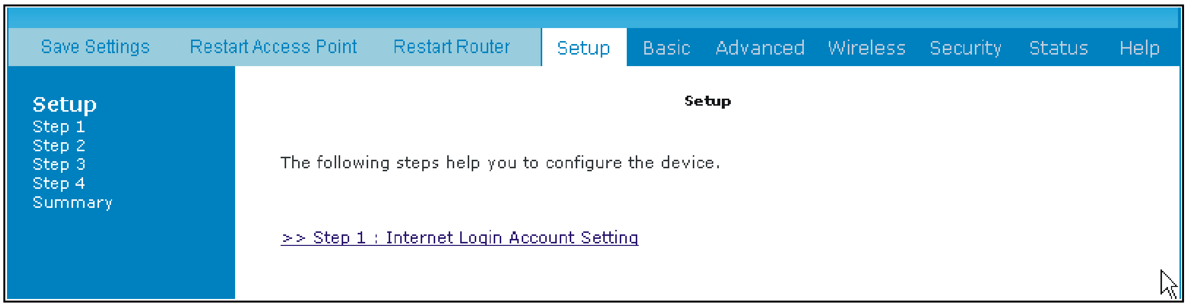
This section will guide you through your ADSL Router's configuration. The ADSL Router is shipped with a standard PPP configuration.

The basic tabs consist of features which are catered for basic users.

4.1 Logging into your ADSL Router

To configure your ADSL Router, open your web browser. You may get an error message at this point; this is normal. Type the default IP address (**192.168.1.1**) or **login.router** on the web address bar.

☞ **NOTE:** Before setting up your ADSL Router, make sure you have followed the easy start guide. You should have your computers configured for DHCP mode and have proxies disabled on your browser. Upon accessing the ADSL Router, if the browser still displays a login redirection screen, you should check your browser's setting and ensure that the JavaScript support is enabled. If the screen shown in Figure 1-4 is not attainable, you must delete your temporary Internet files to clear the web cache.



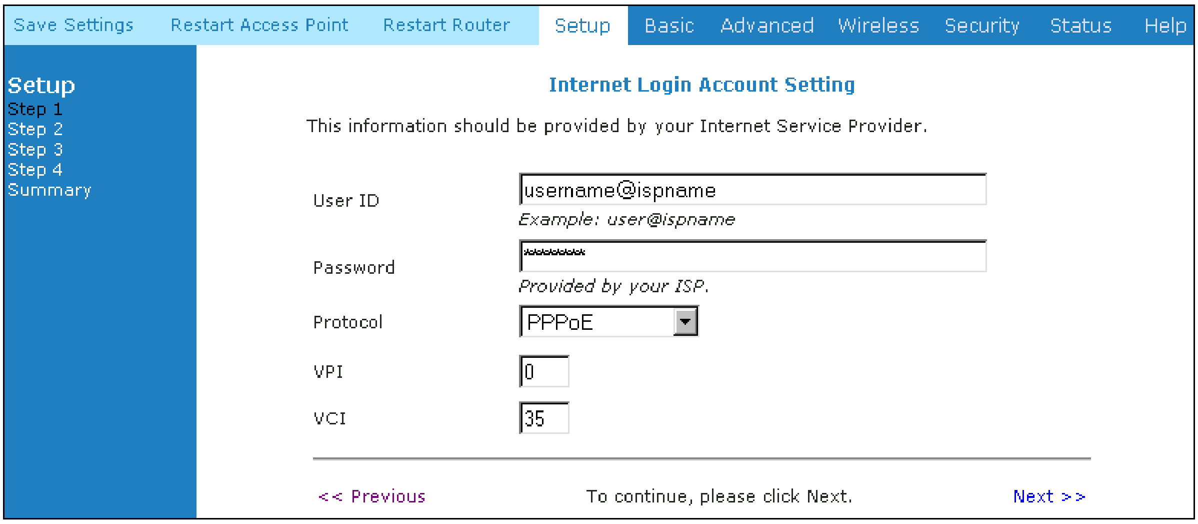
Setup

The following steps help you to configure the device.

>> Step 1 : Internet Login Account Setting

Figure 1-4 : Setup Page

Upon entering the default IP address or the short-cut name (login.router), if the user is logging for the first time, the user will be brought to the "Internet Login Account Setting" page. See Figure 1-5. This page is meant for basic users whom only require easy connectivity to the Internet without worrying about any other advance configuration setting. If you are in doubt for what content to enter for the Protocol, VPI and VCI, please contact your Service Provider for assistance.



Internet Login Account Setting

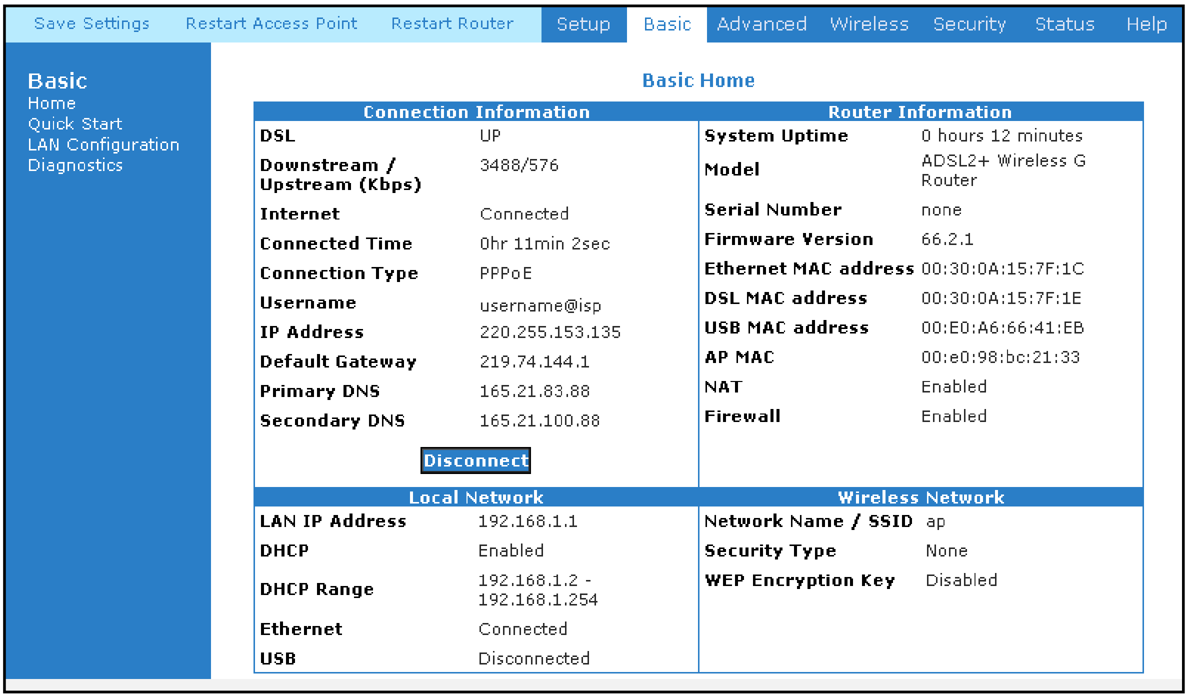
This information should be provided by your Internet Service Provider.

User ID	username@ispname *Example: user@ispname*
Password	******** *Provided by your ISP.*
Protocol	PPPoE
VPI	0
VCI	35

<< Previous   To continue, please click Next.   Next >>

Figure 1-5 : Internet Login Account Setting

For those who have their routers configured, you will be directed to the "Basic Home" page. See Figure 1-6.



Basic Home

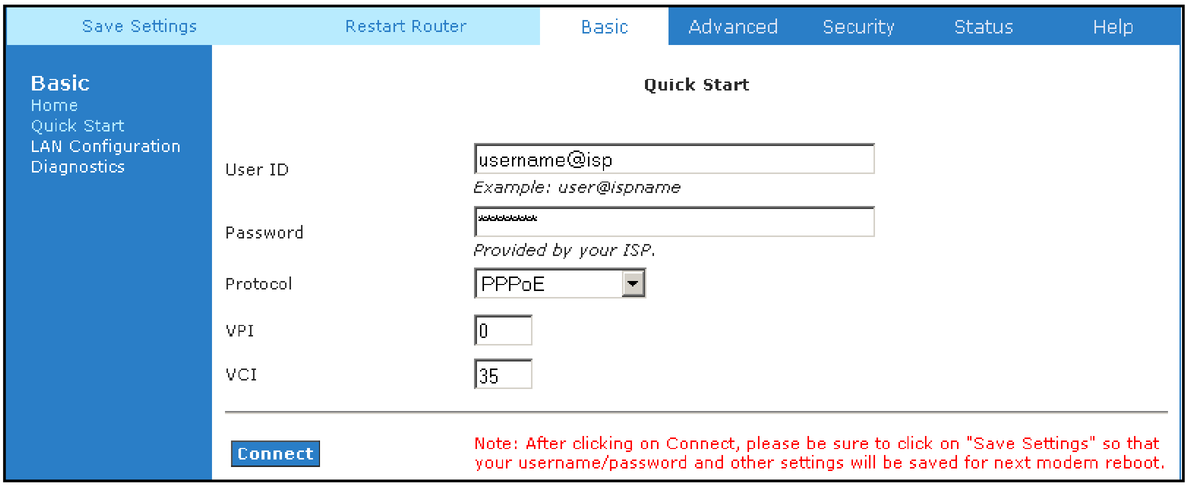
Connection Information		Router Information	
DSL	UP	**System Uptime**	0 hours 12 minutes
Downstream / Upstream (Kbps)	3488/576	**Model**	ADSL2+ Wireless G Router
Internet	Connected	**Serial Number**	none
Connected Time	0hr 11min 2sec	**Firmware Version**	66.2.1
Connection Type	PPPoE	**Ethernet MAC address**	00:30:0A:15:7F:1C
Username	username@isp	**DSL MAC address**	00:30:0A:15:7F:1E
IP Address	220.255.153.135	**USB MAC address**	00:E0:A6:66:41:EB
Default Gateway	219.74.144.1	**AP MAC**	00:e0:98:bc:21:33
Primary DNS	165.21.83.88	**NAT**	Enabled
Secondary DNS	165.21.100.88	**Firewall**	Enabled
Disconnect			

Local Network		Wireless Network	
LAN IP Address	192.168.1.1	**Network Name / SSID**	ap
DHCP	Enabled	**Security Type**	None
DHCP Range	192.168.1.2 - 192.168.1.254	**WEP Encryption Key**	Disabled
Ethernet	Connected		
USB	Disconnected		

Figure 1-6 : Basic Home

4.2 Quick Start

If you have already configured your router and wish to change your current configuration, click on the ‘Quick Start’ link. Figure 1-7 will appear.



Quick Start

User ID: username@isp
Example: user@ispname

Password: ********
Provided by your ISP.

Protocol: PPPoE

VPI: 0

VCI: 35

Note: After clicking on Connect, please be sure to click on "Save Settings" so that your username/password and other settings will be saved for next modem reboot.

Figure 1-7 : Quick Start Page

4.3 LAN / DHCP Configuration

On one side of your ADSL Router, you have your own Local Area network (LAN) connections. This is where you plug in your local computers to the ADSL Router. The ADSL Router is normally configured to automatically provide all the PC's on your network with Internet addresses.

To enable or disable DHCP, click Basic, and then select LAN Configuration. The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the ADSL Router IP address value. For example if the ADSL Router IP address is 192.168.1.1 (default) than the starting IP address must be 192.168.1. 2 (or higher).

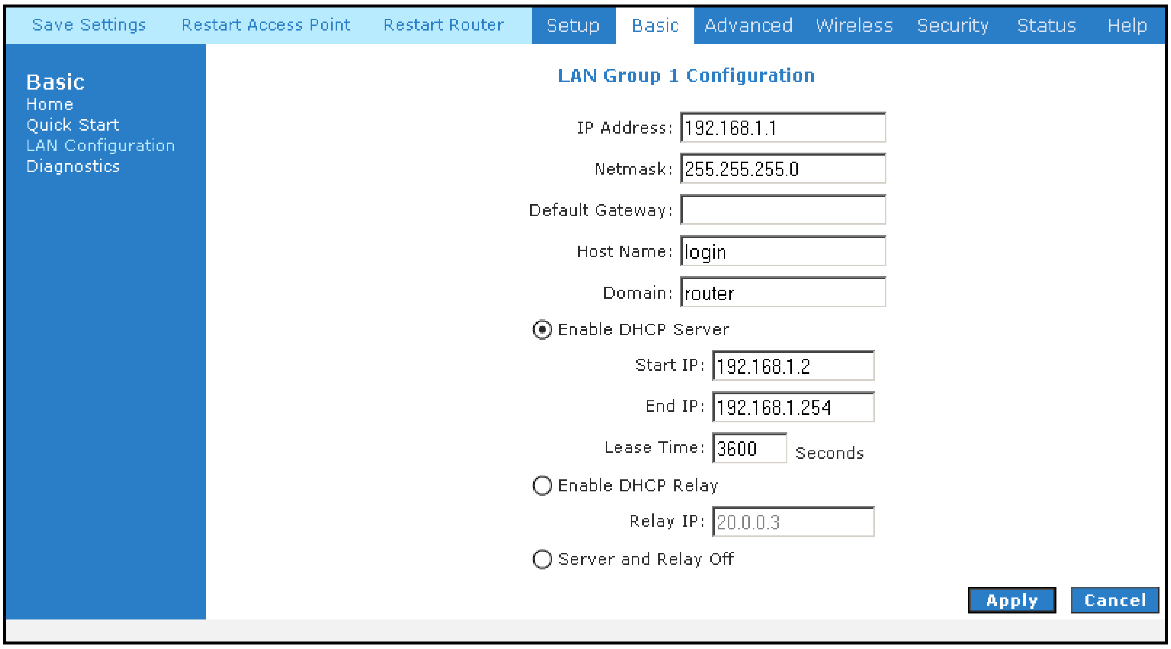
The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254. Hence the max value for our default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this happens you can increase the Ending IP address (to the limit of 255) or reduce the lease time.

The Lease Time is the amount of time a network user will be allowed connection to the ADSL Router with their current dynamic IP address. The amount of time is in units of minutes; the default value is 3600 minutes (60 hours).

Note: If you change the start or end values, make sure the values are still within the same subnet as the gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the ADSL Router if your PC has DHCP enabled.

In addition to the DHCP server feature, the ADSL Router supports the DHCP relay function. When the ADSL Router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the ADSL Router is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

By turning off the DHCP server and relay the network administrator must carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer and your ADSL Router must be on the same subnet as all the other computers. See Figure 1-8**.**



LAN Group 1 Configuration

IP Address: 192.168.1.1

Netmask: 255.255.255.0

Default Gateway:

Host Name: login

Domain: router

● Enable DHCP Server

Start IP: 192.168.1.2

End IP: 192.168.1.254

Lease Time: 3600 Seconds

○ Enable DHCP Relay

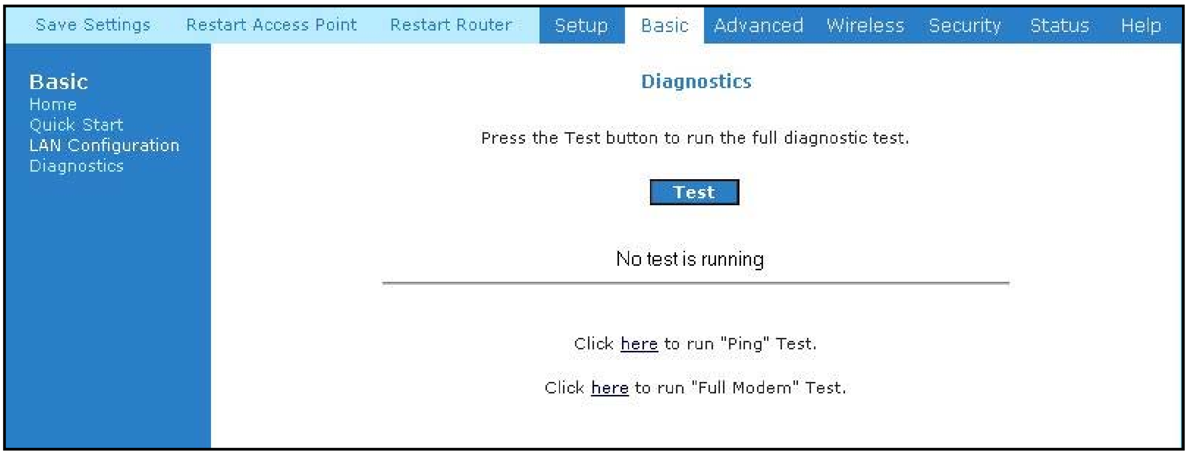
Relay IP: 20.0.0.3

○ Server and Relay Off

Figure 1-8 : LAN / DHCP Configuration

4.4 Diagnostic Test

Diagnostic Test is used for investigating whether the ADSL Router is properly connected to the WAN Network. See Figure 1-9**.** This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link.



Press the Test button to run the full diagnostic test.

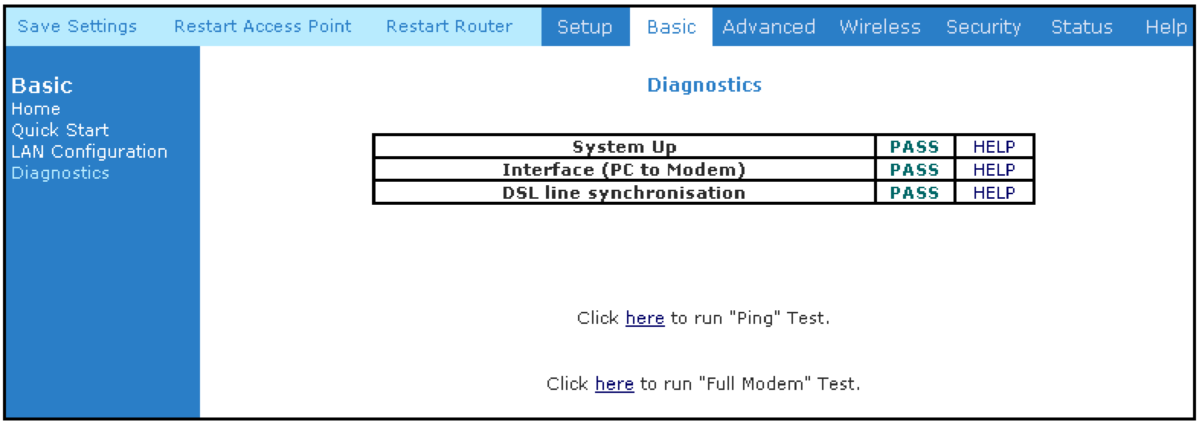
No test is running

Click here to run "Ping" Test.

Click here to run "Full Modem" Test.

Figure 1-9 : Diagnostics Test Screen

After running the Diagnostic Test, the screen will indicate that the portion which pass or fail the test. See Figure 1-10**.** Please click on the **Help** links, which will provide remedy to the problem.



System Up	PASS	HELP
Interface (PC to Modem)	PASS	HELP
DSL line synchronisation	PASS	HELP

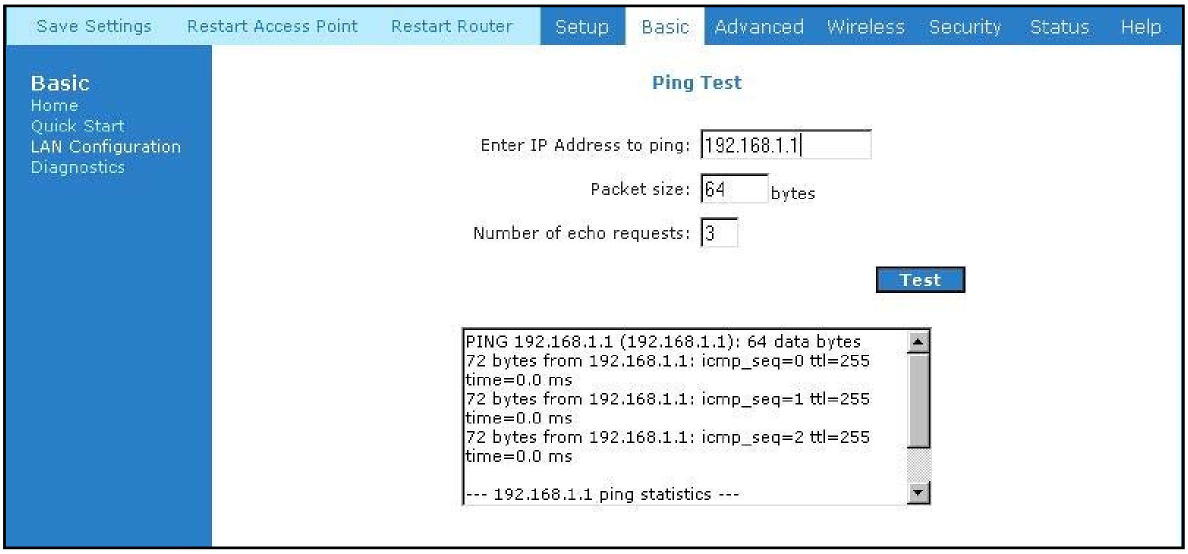
Click here to run "Ping" Test.

Click here to run "Full Modem" Test.

Figure 1-10 : Diagnostics Test Result Screen

4.4.1 Ping Test

Once you have your ADSL Router configured, ensure you can ping the network. Type the target address that you want to ping. If your PC is connected to the ADSL Router via the default DHCP configuration, you should be able to ping the network address 192.168.1.1. See Figure 1-11**.** If your ISP has provided their server address, try to ping the address. If the pings for both the WAN and the LAN sides are complete and you have the proper protocols configured, you should be able to surf the Internet. By default when you select ping test, the ADSL Router will ping itself 3 times. The ADSL Router passed the Ping test; this basically means that the TCP/IP protocol is up and running. If the first Ping test does not pass, the TCP/IP protocol is not loaded for some reason; you should restart the ADSL Router.



Enter IP Address to ping: 192.168.1.1

Packet size: 64 bytes

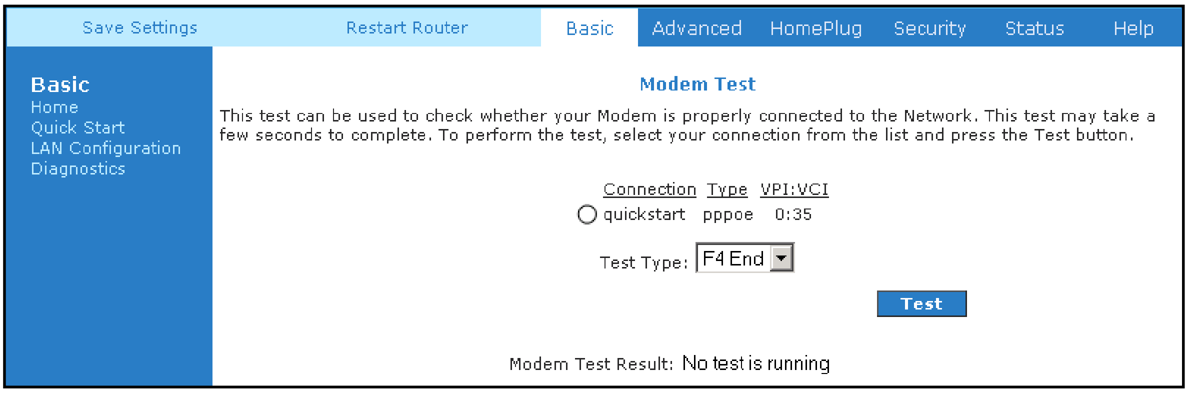
Number of echo requests: 3

```
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255
time=0.0 ms

--- 192.168.1.1 ping statistics ---
```

Figure 1-11 : Ping Test Screen

4.4.2 Modem Test

This test can be used to check whether your Modem is properly connected to the Network. Select your connection from the list and press the **'Test'** button. See Figure 1-12.



This test can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button.

Connection	Type	VPI:VCI
○ quickstart	pppoe	0:35

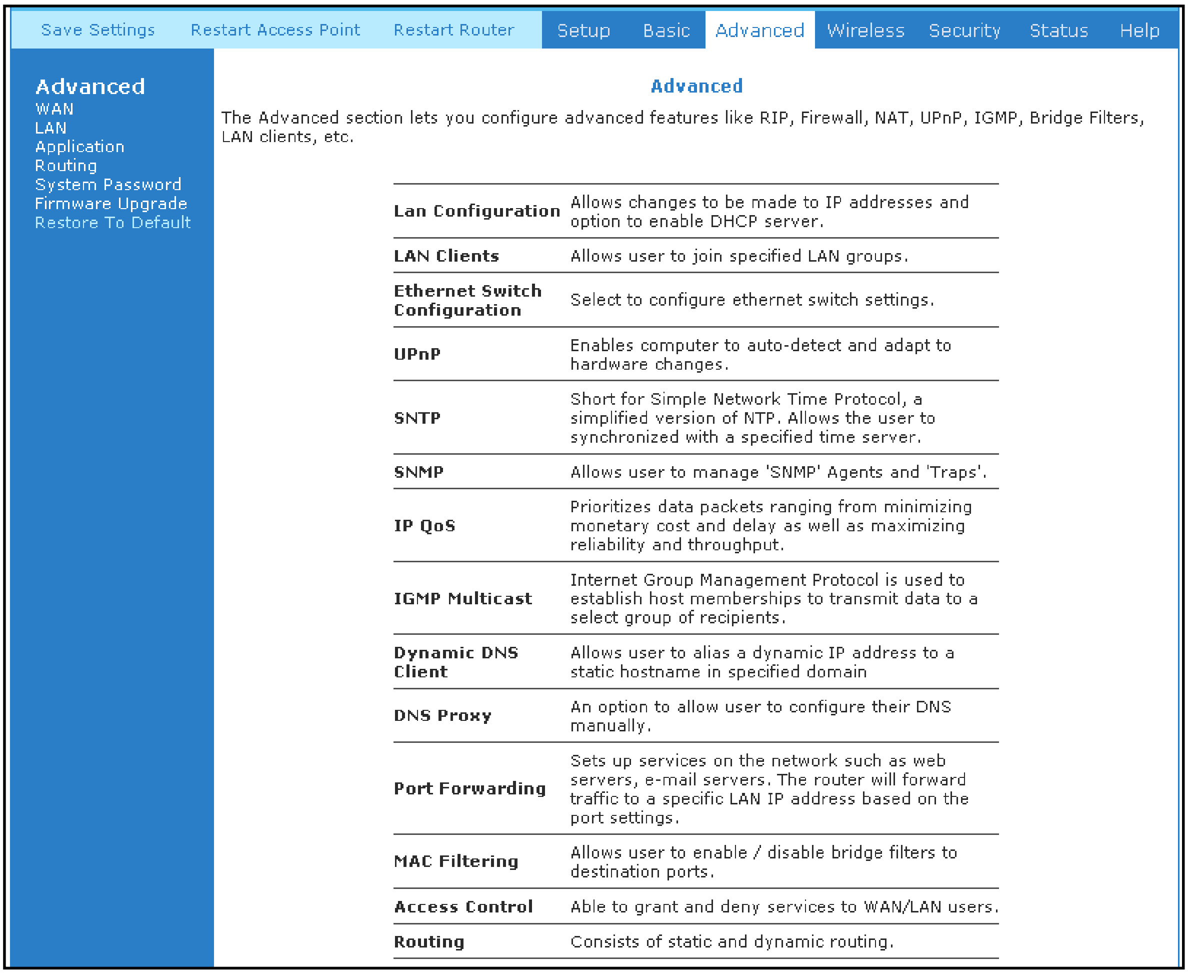
Test Type: F4 End

Modem Test Result: No test is running

Figure 1-12 : Modem Test

4.5 Advanced

This mode is catered for advance users, a brief explanation of the links are listed as shown below. See Figure 1-13**.**



Advanced

The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, LAN clients, etc.

Lan Configuration	Allows changes to be made to IP addresses and option to enable DHCP server.
LAN Clients	Allows user to join specified LAN groups.
Ethernet Switch Configuration	Select to configure ethernet switch settings.
UPnP	Enables computer to auto-detect and adapt to hardware changes.
SNTP	Short for Simple Network Time Protocol, a simplified version of NTP. Allows the user to synchronized with a specified time server.
SNMP	Allows user to manage 'SNMP' Agents and 'Traps'.
IP QoS	Prioritizes data packets ranging from minimizing monetary cost and delay as well as maximizing reliability and throughput.
IGMP Multicast	Internet Group Management Protocol is used to establish host memberships to transmit data to a select group of recipients.
Dynamic DNS Client	Allows user to alias a dynamic IP address to a static hostname in specified domain
DNS Proxy	An option to allow user to configure their DNS manually.
Port Forwarding	Sets up services on the network such as web servers, e-mail servers. The router will forward traffic to a specific LAN IP address based on the port settings.
MAC Filtering	Allows user to enable / disable bridge filters to destination ports.
Access Control	Able to grant and deny services to WAN/LAN users.
Routing	Consists of static and dynamic routing.

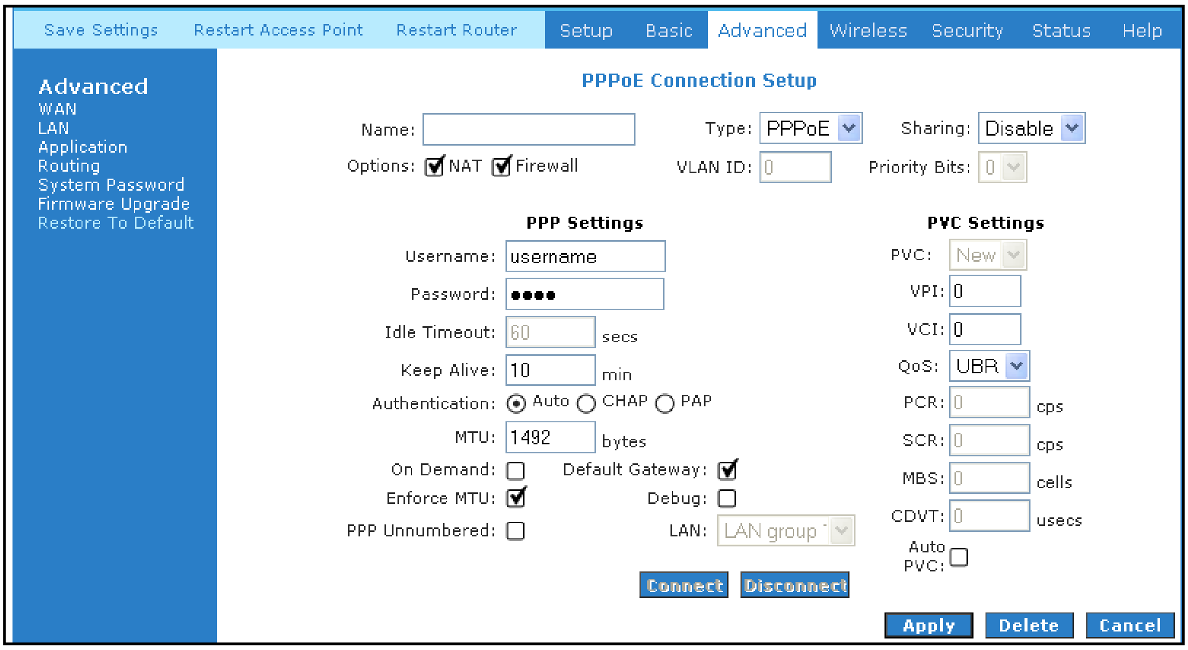
Figure 1-13 : Advanced Screen

4.5.1 WAN Connection

The Wide Area Network (WAN) connection exists on the other side of the ADSL Router, also referred to as a broadband connection. This WAN connection is different for every WAN supplier. Most of the configuration you will perform will be for WAN connection.

4.5.2 New Connection

A new connection is a virtual connection. Your ADSL Router can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly.



PPPoE Connection Setup

Name:
Type: PPPoE
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Username: username
Password: ●●●●
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □
PPP Unnumbered: □
LAN: LAN group

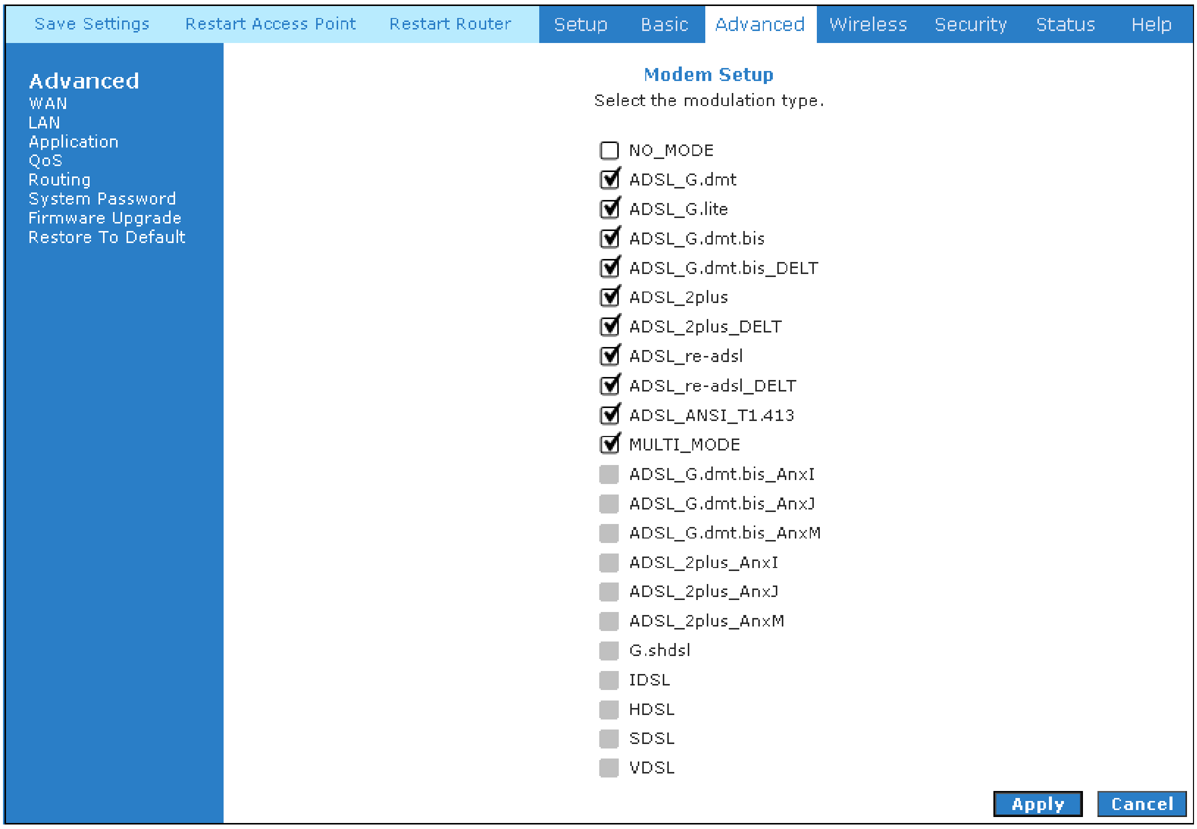
PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Figure 1-14 : New Connection (PPPoE Connection Setup)

4.5.3 ADSL Modulation

To configure the DSL modulation type, Click **WAN** > **ADSL Modulation**. This will bring up the modem setup screen. Leave the default value if you are unsure or the DSL/ISP did not provide this information. In most cases, this screen should not be modified.



Modem Setup

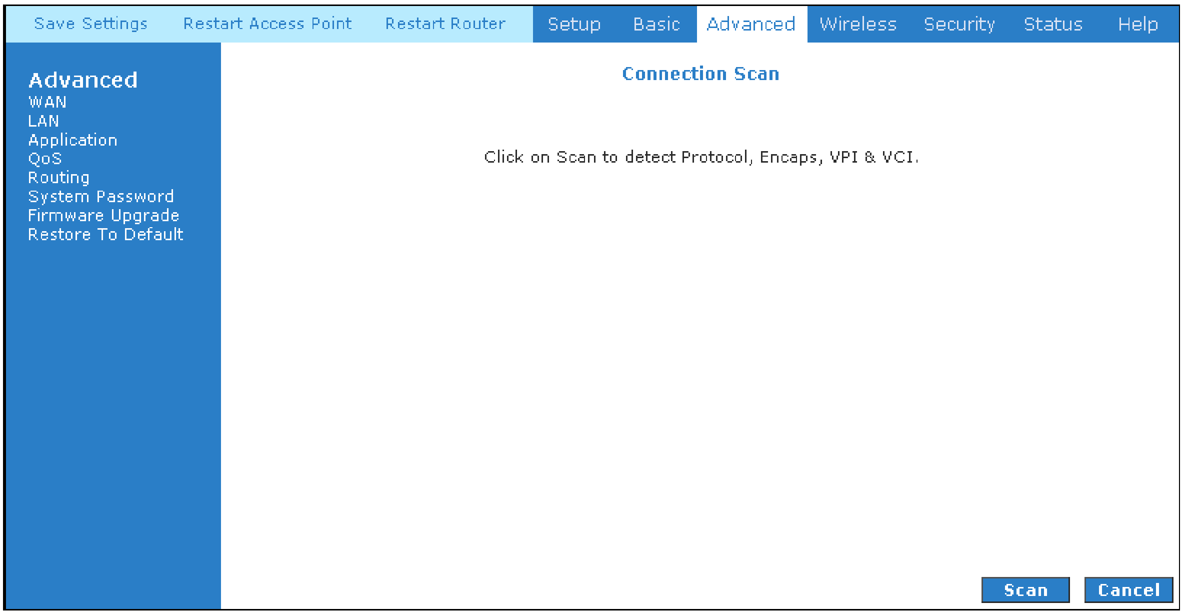
Select the modulation type.

- □ NO_MODE
- ☑ ADSL_G.dmt
- ☑ ADSL_G.lite
- ☑ ADSL_G.dmt.bis
- ☑ ADSL_G.dmt.bis_DELT
- ☑ ADSL_2plus
- ☑ ADSL_2plus_DELT
- ☑ ADSL_re-adsl
- ☑ ADSL_re-adsl_DELT
- ☑ ADSL_ANSI_T1.413
- ☑ MULTI_MODE
- □ ADSL_G.dmt.bis_AnxI
- □ ADSL_G.dmt.bis_AnxJ
- □ ADSL_G.dmt.bis_AnxM
- □ ADSL_2plus_AnxI
- □ ADSL_2plus_AnxJ
- □ ADSL_2plus_AnxM
- □ G.shdsl
- □ IDSL
- □ HDSL
- □ SDSL
- □ VDSL

Figure 1-15 : ADSL Modulation (Modem Setup)

4.5.4 Connection Scan

This feature helps users to detect the PVC settings provided by the ISP. Before the router can begin scanning the connection, the telephone line has to be plugged into the router. Click on **Scan** to begin. See Figure 1-16**.**



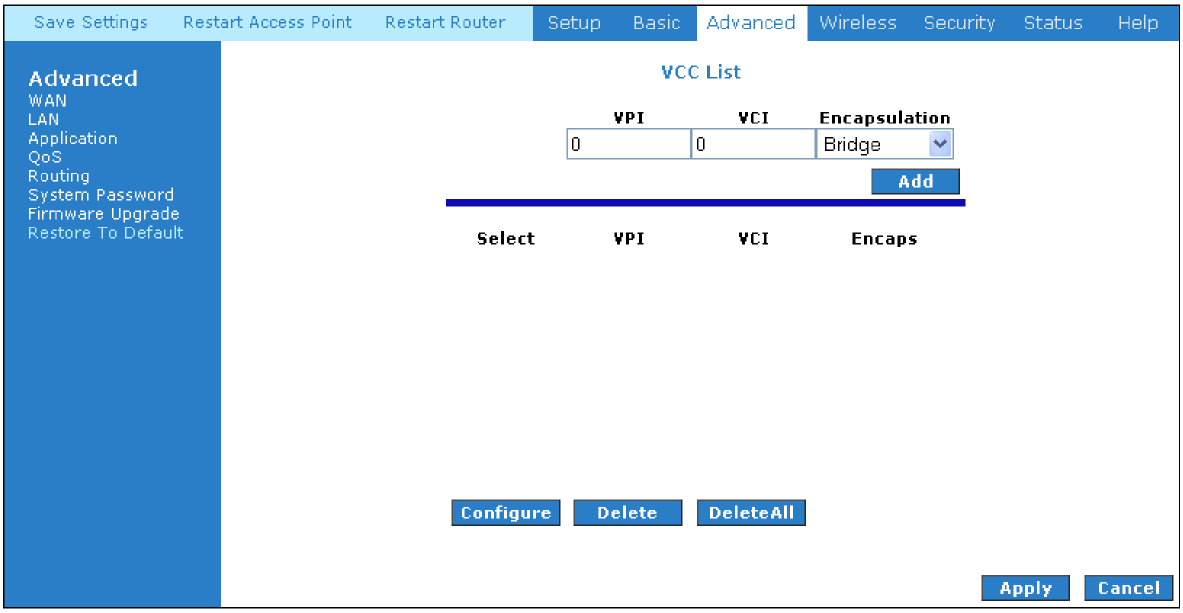
Connection Scan

Click on Scan to detect Protocol, Encaps, VPI & VCI.

Figure 1-16 : Connection Scan

4.5.5 VCC List

Users can configure multiple PVC settings using the VCC List feature. A maximum of 8 settings can be configured. See Figure 1-17.



VCC List

VPI	VCI	Encapsulation
0	0	Bridge

Select	VPI	VCI	Encaps

Figure 1-17 : VCC List

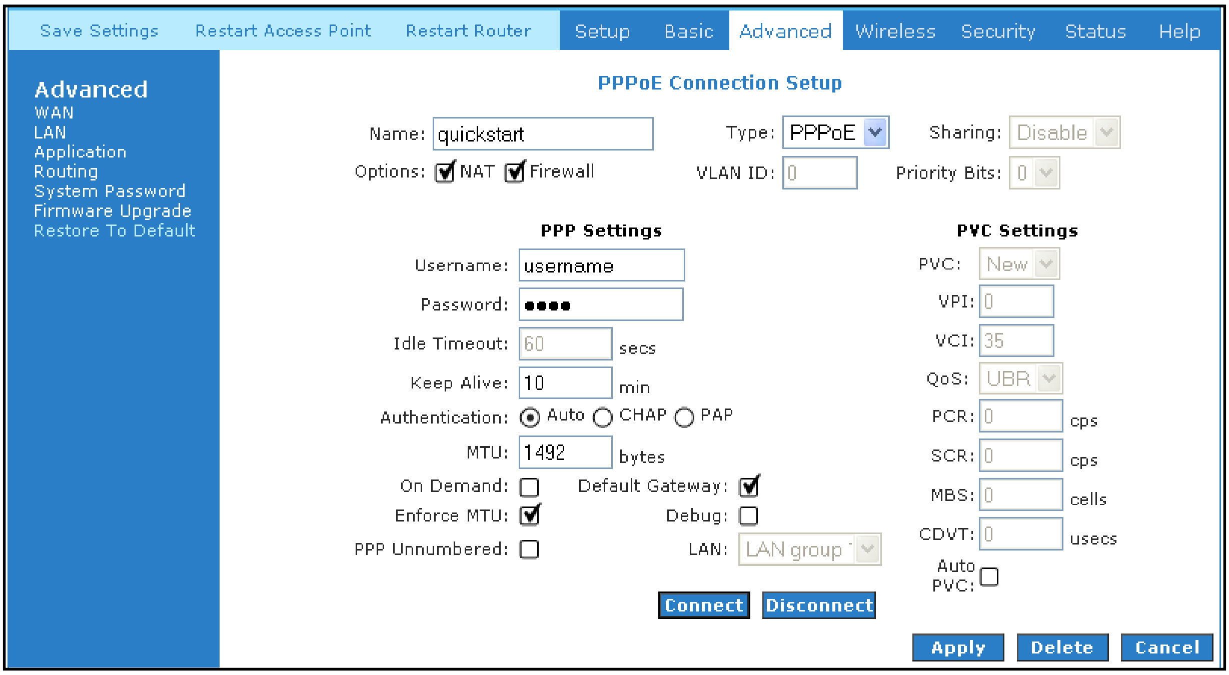
4.5.6 Quickstart

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users.

To configure the gateway for PPPoE, click on Advanced. Under WAN, select New Connection. The default PPPoE connection setup is displayed. At the Type field select PPPoE and the PPPoE connection setup page is displayed. Give your PPPoE connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called quickstart. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these. In this case the DSL service provider is using 0, 100. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information. See Figure 1-18.

Following is a description of the different options:

1. Username: The username for the PPPoE access; this is provided by your DSL service provider or your ISP.
2. Password: The password for the PPPoE access; this is provided by your DSL service provider or your ISP.
3. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
4. Idle Timeout: Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.
5. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
6. Enforce MTU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to PPP MTU.



PPPoE Connection Setup

Name: quickstart
Type: PPPoE
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Username: username
Password: ●●●●
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □
PPP Unnumbered: □
LAN: LAN group 1

PVC Settings

PVC: New
VPI: 0
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Figure 1-18 : Quickstart (PPPoE Connection Setup)

4.5.7 LAN Configuration

You can change the ADSL Router's IP address by, clicking **LAN**, and then **LAN Configuration**. Select the options from LAN group 1 and click **Configure**.

Your ADSL Router's default IP address and subnet mask are 192.168.1.1/255.255.255.0; this subnet mask will allow the ADSL Router to support 254 users. If you want to support a larger number of users you can change the subnet mask; but remember that the DHCP server is defaulted to only give out 255 IP addresses. Further remember that if you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet. The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.

The hostname can be any alphanumeric word that does not contain spaces. The domain name is used to in conjunction with the host name to uniquely identify the gateway. To access the ADSL Router's web pages, the user can type 192.168.1.1 (the default IP address) or type login.router. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). Refer to Figure 1-19.

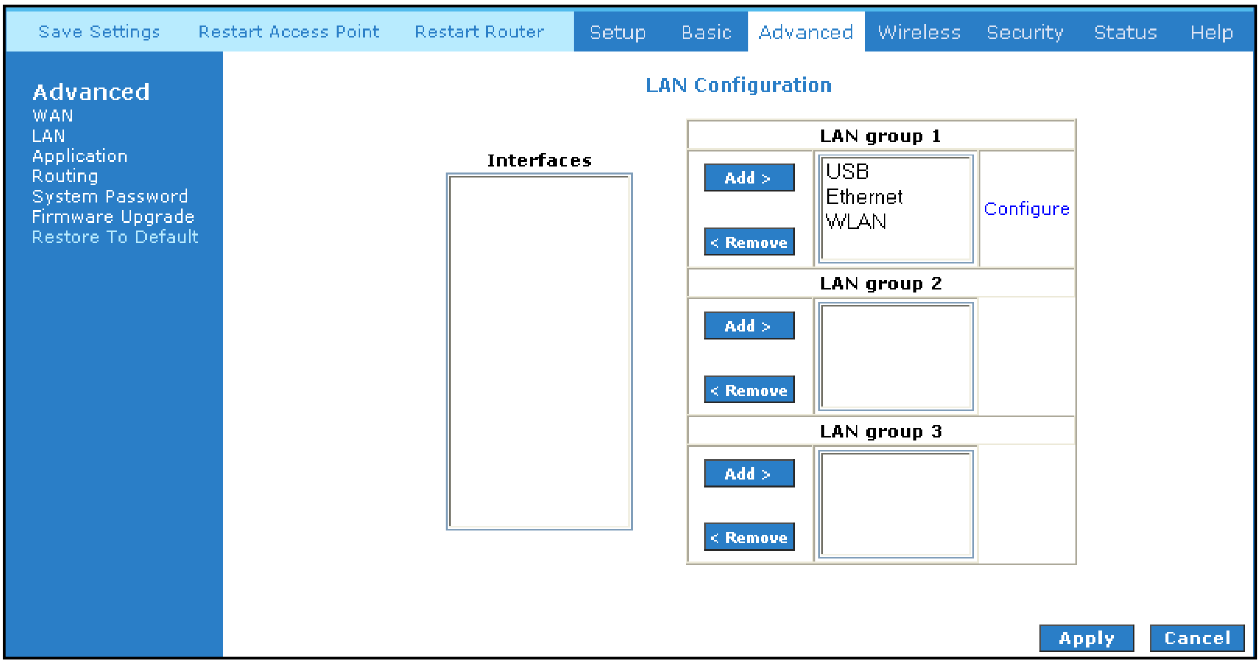
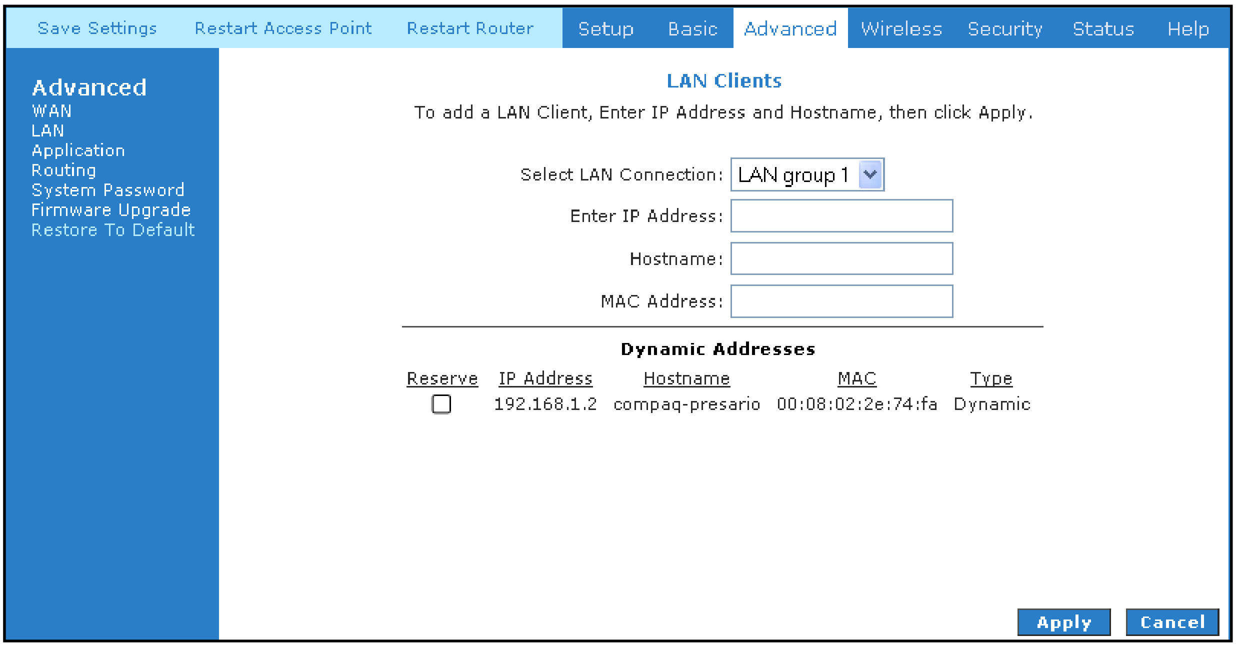


Figure 1-19 : LAN Configuration

4.5.8 LAN Clients

To add a LAN client, select **LAN clients** option under **LAN**. If DHCP was enabled in the configuration, all DHCP clients are automatically assigned with IP address. If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added, you can apply Port Forwarding and Access Control rules to this IP address.



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Dynamic Addresses

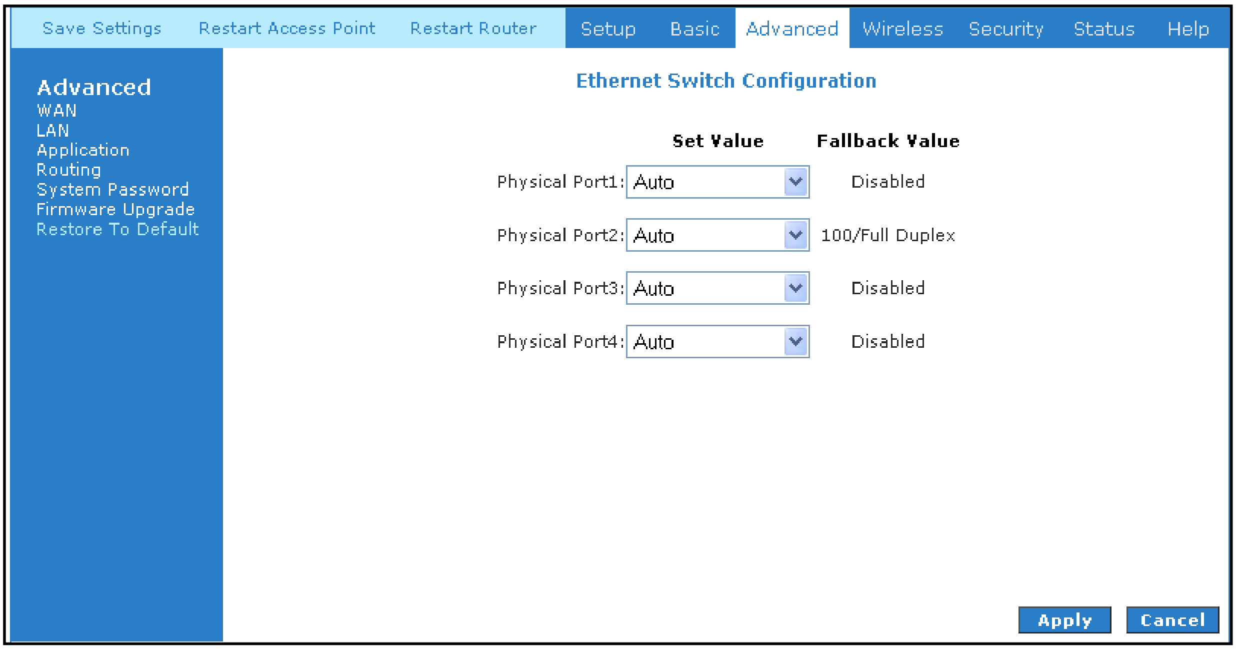
Reserve	IP Address	Hostname	MAC	Type
□	192.168.1.2	compaq-presario	00:08:02:2e:74:fa	Dynamic

Figure 1-20 : LAN Clients

4.5.9 Ethernet Switch Configuration

The IGMP Snooping prevents the switch from flooding the LAN ports with multicast frames, and will instead direct them to the CPU port for processing. Users are able to specify connection speed and set their values accordingly from the following available options. See Figure 1-21.

- Auto
- 10/Half Duplex
- 10/Full Duplex
- 100/Half Duplex
- 100/Full Duplex



Ethernet Switch Configuration

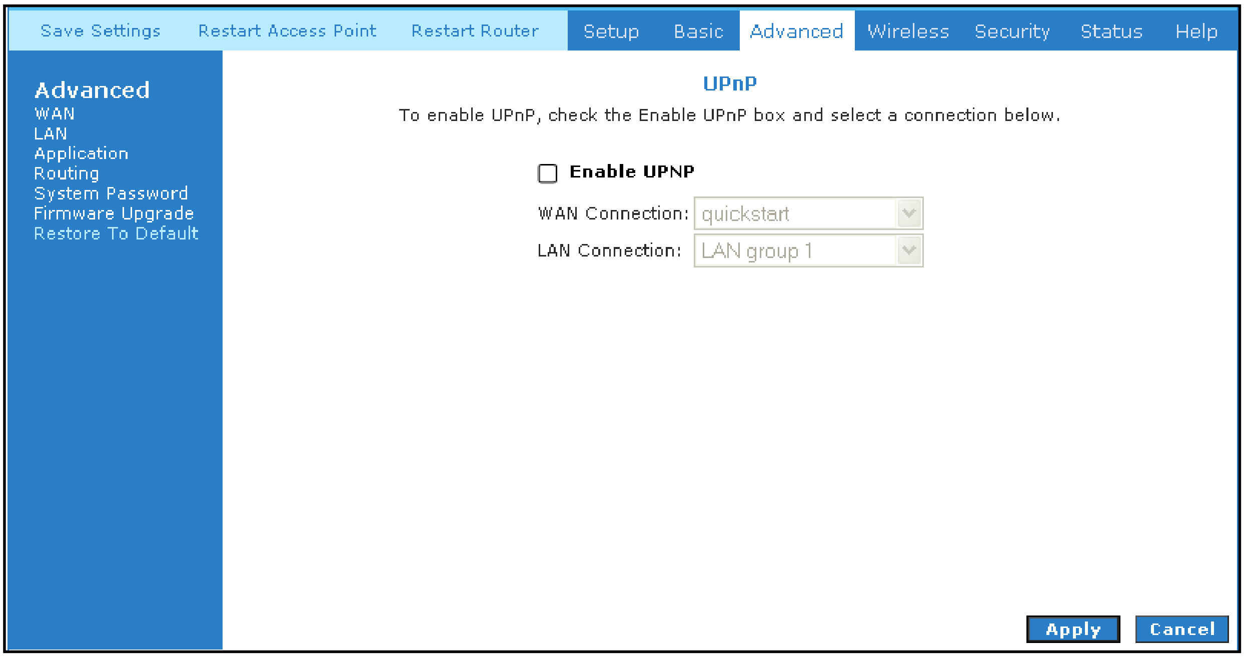
	Set Value	Fallback Value
Physical Port1:	Auto	Disabled
Physical Port2:	Auto	100/Full Duplex
Physical Port3:	Auto	Disabled
Physical Port4:	Auto	Disabled

Figure 1-21 : Ethernet Switch Configuration

4.5.10 Application (UPnP)

UPnP, NAT and Firewall Traversal allow traffic to pass-thru the ADSL Router for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over, which the incoming traffic will be present, for example the default Internet connection.

To enable UPnP, you must first have a WAN connection configured. Once a WAN connection is configured, click **Advanced** and under **Application**, select **UPnP**. You must enable UPnP and then select which connection will utilize UPnP. See Figure 1-22.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

☐ **Enable UPNP**

WAN Connection: quickstart

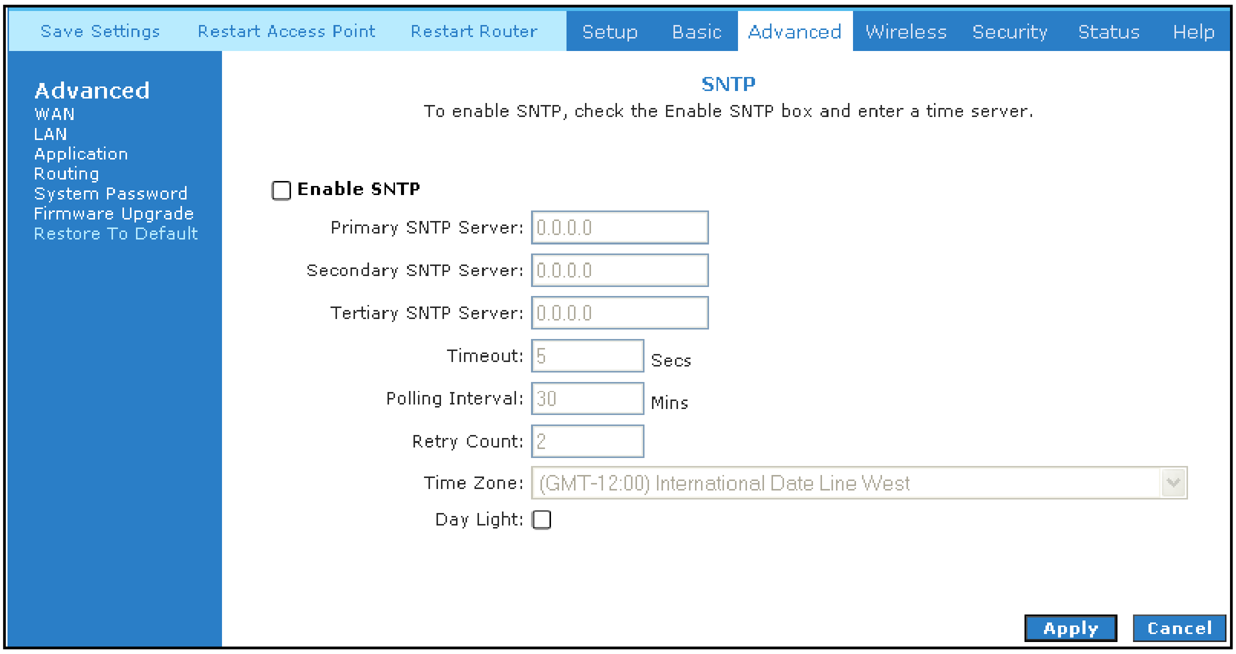
LAN Connection: LAN group 1

Figure 1-22 : UPnP

4.5.11 SNTP

SNTP (Simple Network Timing Protocol) is a protocol used to synchronize the system time to the public SNTP servers. When the SNTP feature is enabled, your router will start querying for the time clock information from the primary SNTP server. If it fails to get a valid response within the "timeout" period, it will try for "retry" number of times, before moving to the Secondary SNTP server. If it fails to get a valid response from Secondary STNP server within valid retry times, it starts querying Tertiary SNTP server. If it fails to get a valid response from all the servers, then the program stops. When a valid response is received from one of the server, the program sleeps for "Polling_interval" amount of minutes, before starting the whole process again. Use the following procedures to enable SNTP.

1. Check Enable SNTP.
2. Primary SNTP Server - The IP address or the host name of the primary SNTP server.
3. Secondary SNTP Server - The IP address or the host name of the secondary SNTP server.
4. Tertiary SNTP Server - The IP address or the host name of the tertiary SNTP server.
5. Timeout - If the router failed to connect to a SNTP server within the 'Timeout' period, it will retry the connection.
6. Polling Interval - Time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
7. Retry Count - The number of times the router will try to connect to an SNTP server before it try to connect to the next server in line.
8. Time Zone - The time zone of the router.
9. Day Light - Check/uncheck this option to enable/disable day light saving. See Figure 1-23.



SNTP

To enable SNTP, check the Enable SNTP box and enter a time server.

□ Enable SNTP

Primary SNTP Server: 0.0.0.0

Secondary SNTP Server: 0.0.0.0

Tertiary SNTP Server: 0.0.0.0

Timeout: 5 Secs

Polling Interval: 30 Mins

Retry Count: 2

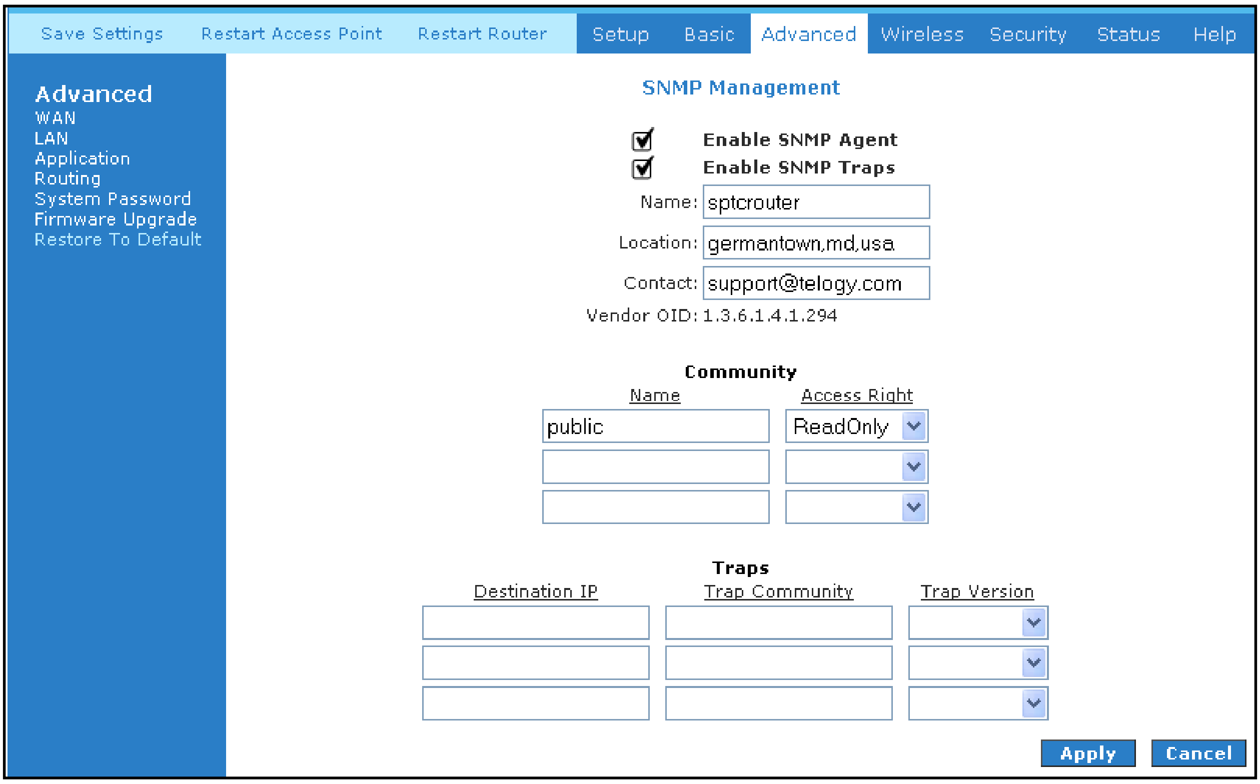
Time Zone: (GMT-12:00) International Date Line West

Day Light: □

Figure 1-23 : SNTP

4.5.12 SNMP

SNMP (Simple Network Management Protocol) is a troubleshooting and management protocol, which uses the UDP protocol on port 161 to communicate between clients and servers. SNMP uses a manager MIB (management information base) agent solution to fulfill the network management needs. The agent is a separate station that can request data from an SNMP agent in each of the different managed system in the network. The agent uses the MIBs as dictionaries of manageable objects. Each SNMP-managed device has at least one agent that can respond to the queries from the NMS. The SNMP agent supports GETS, SETS, and TRAPS for 4 groups with MIB-II: System, Interface, IP, and ICMP. The SNMP agent supports three-community names authentication. See Figure 1-24.



SNMP Management

☑ Enable SNMP Agent

☑ Enable SNMP Traps

Name: sptcrouter

Location: germantown,md,usa

Contact: support@telogy.com

Vendor OID: 1.3.6.1.4.1.294

Community

Name	Access Right
public	ReadOnly

Traps

Destination IP	Trap Community	Trap Version

Figure 1-24 : SNMP Management

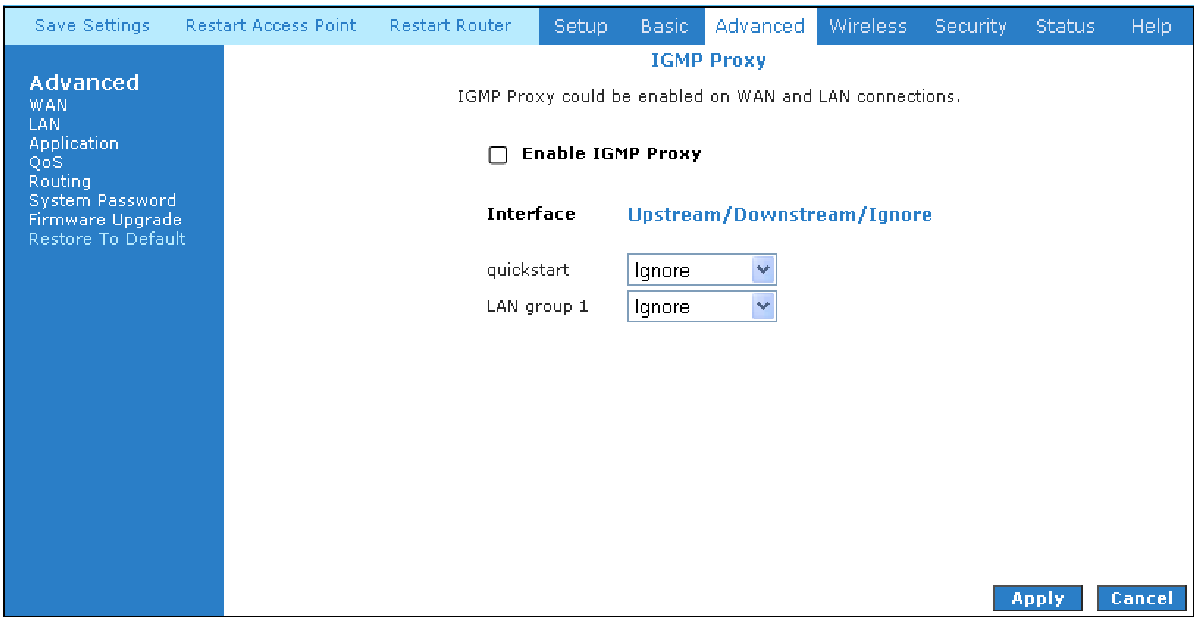
4.5.13 IGMP Proxy

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.
- Non-group members may send UDP datagrams to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your router supports IGMP proxy that handles IGMP messages. When enabled, your router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.



IGMP Proxy

IGMP Proxy could be enabled on WAN and LAN connections.

□ Enable IGMP Proxy

Interface Upstream/Downstream/Ignore

quickstart Ignore

LAN group 1 Ignore

Figure 1-25 : IGMP Proxy

IGMP Proxy page (Figure 1-25) allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- Upstream: The interface that IGMP requests from hosts are sent to the multicast router.

- Downstream: The interface data from the multicast router are sent to hosts in the multicast group database.

- Ignore: No IGMP request nor data multicast are forwarded.

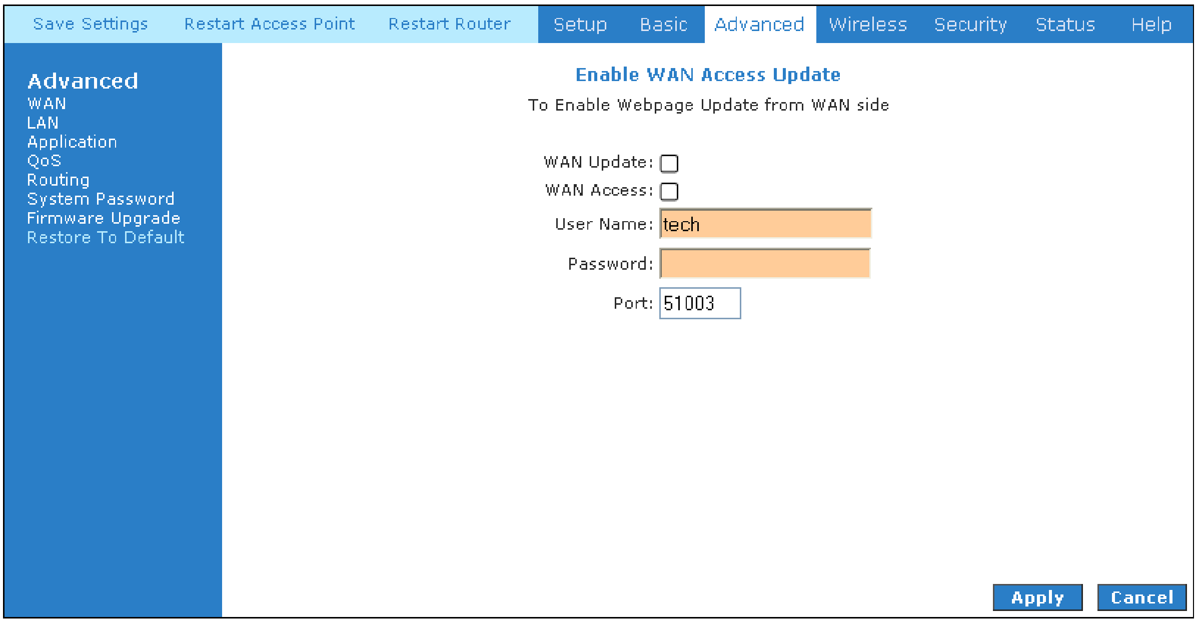
You can perform one of the two options:

1. Configure one or more WAN interface as the upstream interface.

2. Configure one or more LAN interface as the upstream interface.

4.5.14 TR-068 WAN Access

The TR-068 WAN Access page (Figure 1-26) enables you to give temporary permission to someone (such as technical support staff) to be able to access your router from the WAN side. From the moment the account is enabled, the user is expected to log in within 20 active minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.



Enable WAN Access Update

To Enable Webpage Update from WAN side

WAN Update: □

WAN Access: □

User Name: tech

Password:

Port: 51003

Figure 1-26 : TR-068 WAN Access

To create a temporary user account for a remote access to your router, follow the procedure below.

1. Check **WAN Update** to enable write privilege of the router.

2. Check **WAN Access** to enable read privilege of the router.

3. Enter a user name and password in the User Name and Password fields.

4. Enter a port number In the Port field (for example, 51003).

5. Click **Apply** to temporarily activate the settings on the page.

Note—The changes take effect when you click Apply; however, if the router configuration is not saved, these changes will be lost upon reboot.

6. To make the change permanent, click Save Settings.

7. To access your router remotely, enter the following in the URL:

http(s)://WAN IP of router:Port Number

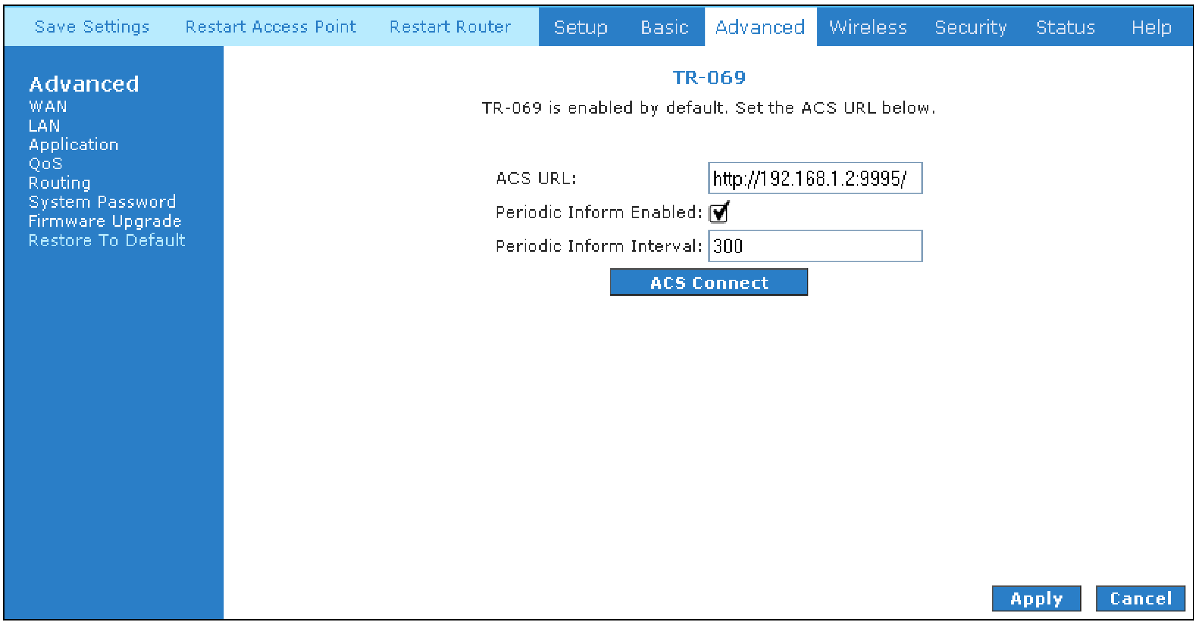
4.5.15 TR-069

TR-069 is CPE Management Protocol from WAN side, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

The CPE WAN Management Protocol is intended to support a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

Figure 1-27 shows the default TR-069 page, which is accessed by clicking the TR-069 link on the Advanced page. The TR-069 page allows you to set up connection parameters and may not be seen by the end user.



TR-069

TR-069 is enabled by default. Set the ACS URL below.

ACS URL: http://192.168.1.2:9995/

Periodic Inform Enabled: ☑

Periodic Inform Interval: 300

Figure 1-27 : TR-069

Follow the procedure below to configure parameters related to TR-069.

1. Leave the default URL in the **ACS URL** field.
2. Check **Periodic Inform Enabled** and enter a value in the **Periodic Inform Interval** field.

OR

Click **ACS Connect** to manually connect to the ACS. Once a connection is established, the ACS can update all three fields: **ACS URL**, **Periodic Inform Enabled**, and **Periodic Inform Interval**.

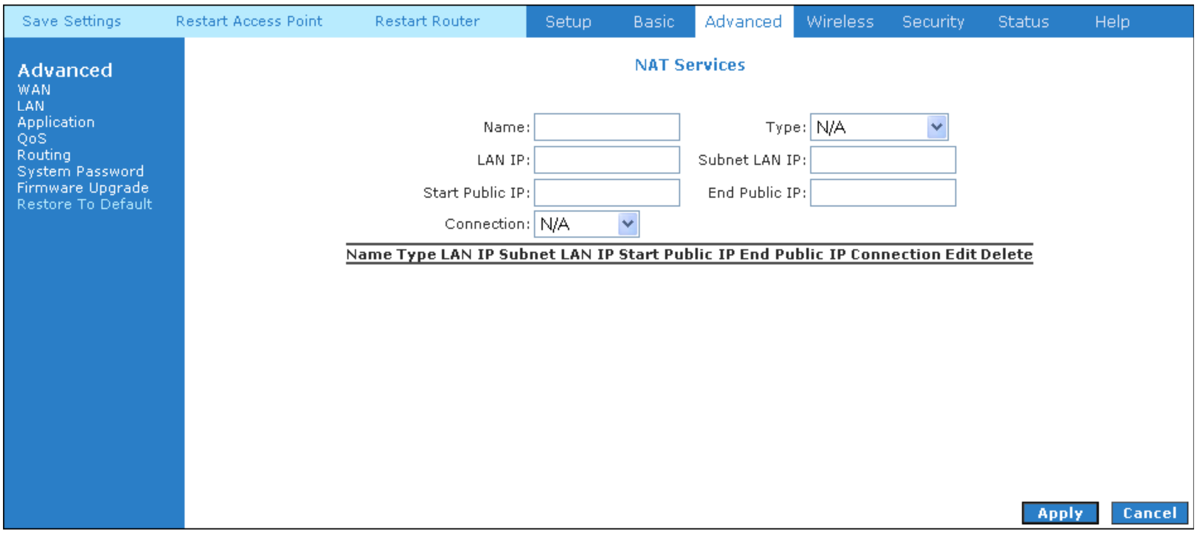
3. Click **Apply** to temporarily activate the settings.

Note—The changes take effect when you click **Apply**; however, if the router configuration is not saved, these changes will be lost upon reboot.

4. To make the change permanent, click **Save Settings**.

4.5.16 NAT Services

If the user has more than one public IP address assigned by the ISP, these additional IP addresses can be used to map to servers on the LAN. One public IP address will be used to provide Internet access to the LAN PCs via NAT, serving as the primary IP address of the router. The rest will be mapped to servers on the LAN. Refer to Figure 1-28.



NAT Services

Name:

Type: N/A

LAN IP:

Subnet LAN IP:

Start Public IP:

End Public IP:

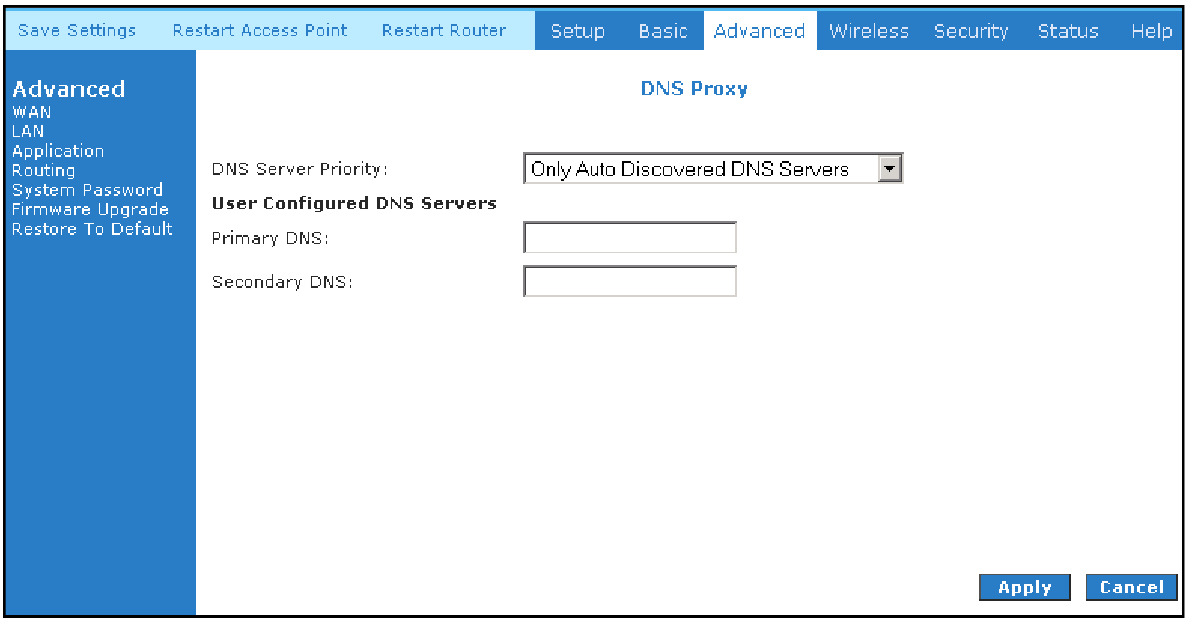
Connection: N/A

Name	Type	LAN IP	Subnet LAN IP	Start Public IP	End Public IP	Connection	Edit	Delete

Figure 1-28 : NAT Services

4.5.17 DNS Proxy

This feature allows the user to select the (Domain Name Server) DNS Server Priority as well as enter IP addresses for primary DNS and secondary DNS. See Figure 1-29.



DNS Proxy

DNS Server Priority: Only Auto Discovered DNS Servers

User Configured DNS Servers

Primary DNS:

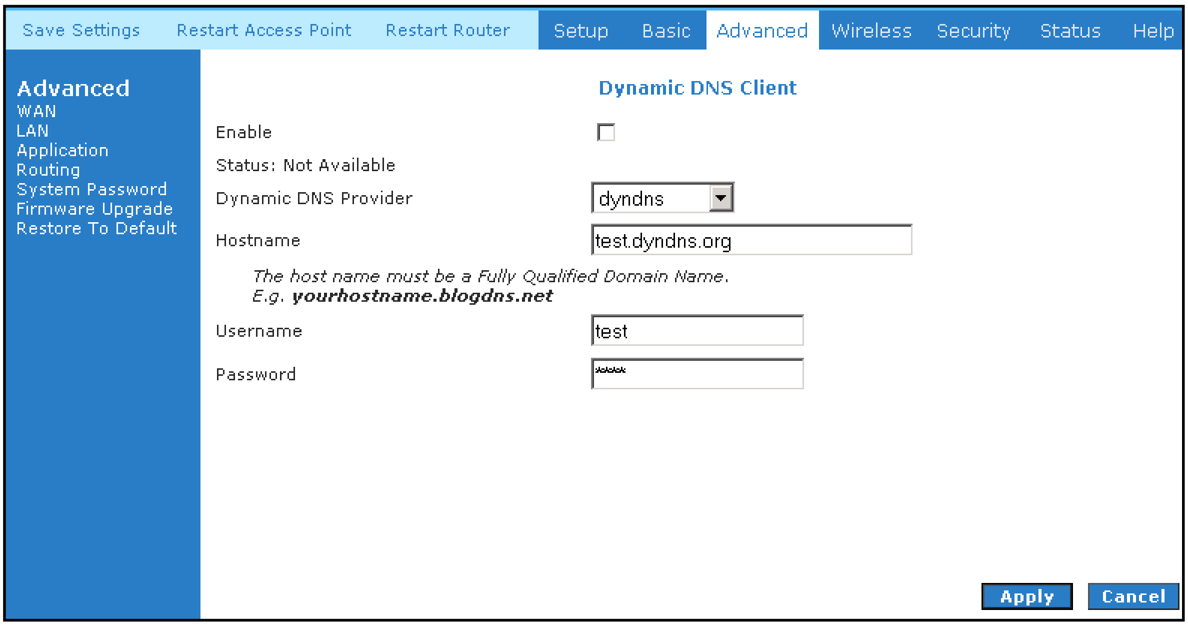
Secondary DNS:

Figure 1-29 : DNS Proxy

4.5.18 Dynamic DNS Client

Dynamic DNS allows the user to register with a Dynamic DNS Provider as listed. The dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services. See Figure 1-30.

Note: The Username/Password entered should be similar to the Username/Password you have specified during the registration of the DNS hostname.



Dynamic DNS Client

Enable □

Status: Not Available

Dynamic DNS Provider: dyndns

Hostname: test.dyndns.org

The host name must be a Fully Qualified Domain Name.
E.g. ***yourhostname.blogdns.net***

Username: test

Password: ****

Figure 1-30 : Dynamic DNS Client

4.5.19 Easy Connect Configuration

Easy Connect feature allow user to surf web with ease without the need to changes default configuration setting, i.e. TCP/IP, Proxy, DNS of user's PC. See Figure 1-31.

There are 4 features on Easy Connect:

1. **Auto IP:** All valid TCP/IP setting on user's PC can surf web via ADSL modem routers without the need to change the IP address to the same subnet as the router or set to "Obtain an IP address automatically".
2. **Auto DNS:** Any DNS IP address set at user's PC irregardless whether the address is valid or invalid DNS, Auto DNS still allow user's PC to surf the web.
3. **Auto Proxy:** Any valid **Private IP** proxy setting with any port number, ie 1234 on the web browser such as Internet Explorer, Auto Proxy still allow PC to surf the web. Any **Public IP** proxy setting will assume the proxy is valid and hence Auto Proxy function will not take place.

NOTE: The port number to be used must be specified in both the web browser and the Auto Proxy Ports.

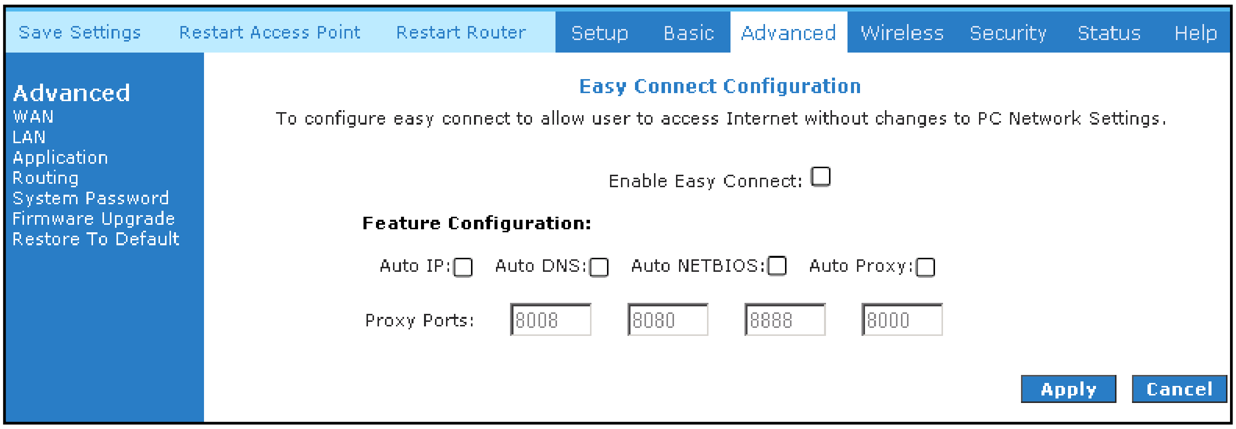
Private IP Ranges

Class A: 10.0.0.0 ~ 10.255.255.255

Class B: 172.16.0.0 ~ 172.31.255.255

Class C: 192.168.0.0 ~ 192.168.255.255

4. **Auto NetBIOS:** It allows proxy server to use any NetBIOS name which the Auto NetBIOS still allow PC to surf the web with a condition that the router gateway **MUST** be in Private IP Ranges.



Easy Connect Configuration

To configure easy connect to allow user to access Internet without changes to PC Network Settings.

Enable Easy Connect: □

Feature Configuration:

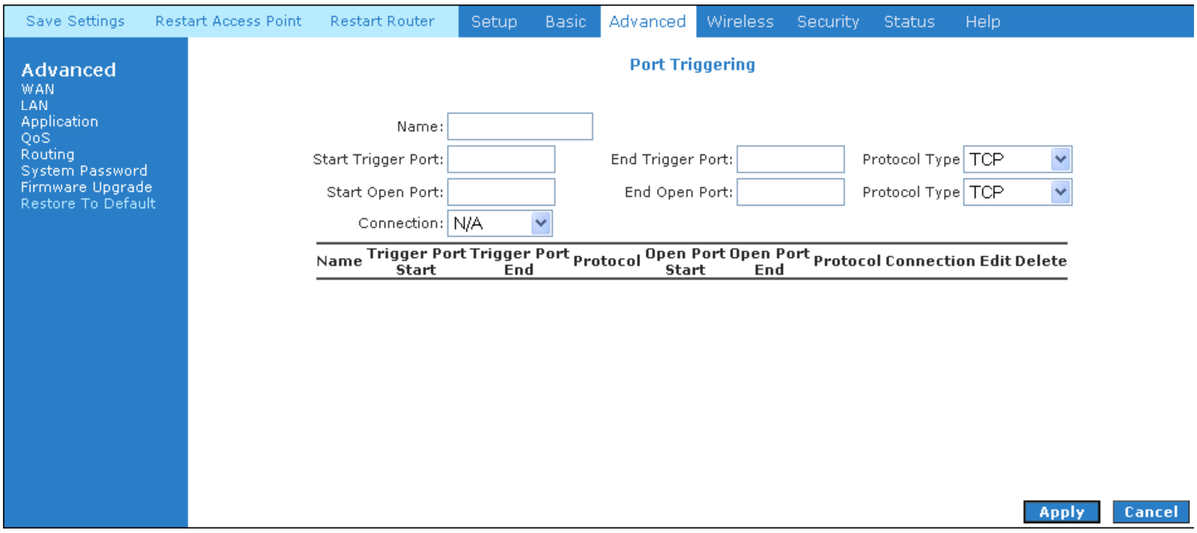
Auto IP: □ Auto DNS: □ Auto NETBIOS: □ Auto Proxy: □

Proxy Ports: 8008 8080 8888 8000

Figure 1-31 : Easy Connect Configuration

4.5.20 Port Triggering

Port triggering is a specialized form of port forwarding which enables computers behind NAT to be accessed. It triggers open an incoming port when a client on the LAN makes an outgoing connection to a predetermined port on a server. Refer to Figure 1-32.



Port Triggering

Name:					
Start Trigger Port:		End Trigger Port:		Protocol Type	TCP
Start Open Port:		End Open Port:		Protocol Type	TCP
Connection:	N/A				

Name	Trigger Port Start	Trigger Port End	Protocol	Open Port Start	Open Port End	Protocol	Connection	Edit	Delete

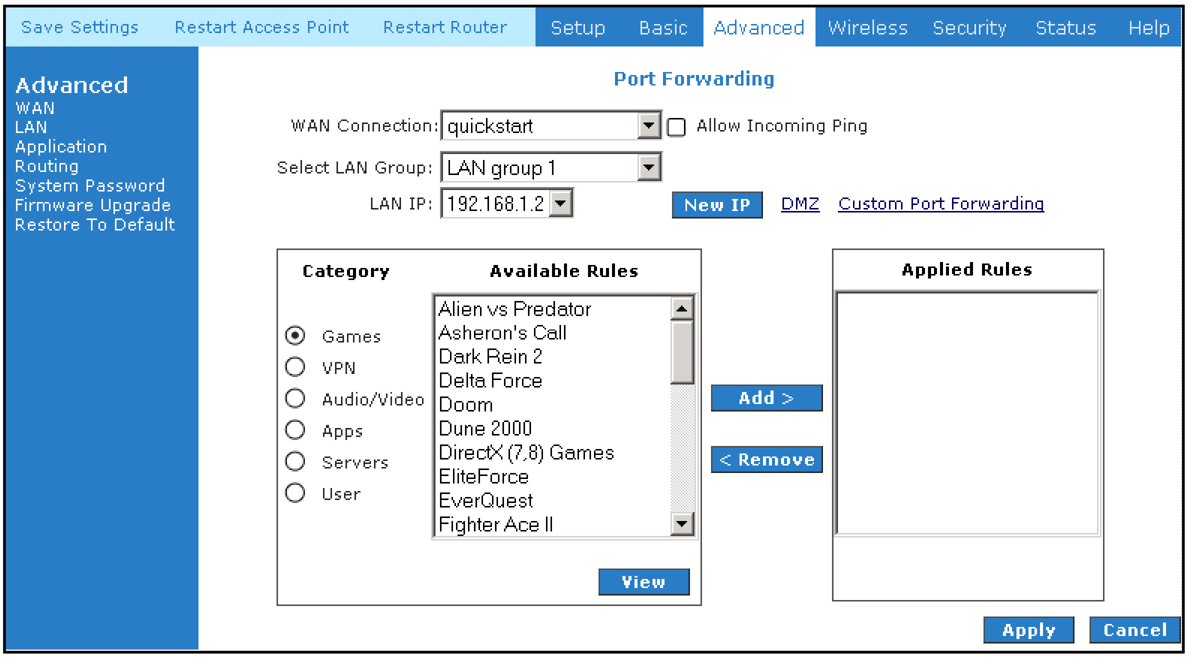
Figure 1-32 : Port Triggering

4.5.21 Port Forwarding

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. When users send this type of request to your network via the Internet, the ADSL Router will forward those requests to the appropriate PC. Port forwarding can be used with DHCP assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a Netmeeting server, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding will translate the WAN IP address into a LAN IP address.

To configure a service, game, or other application select the external connection (for example the Internet connection), from the Home screen, click Advanced and under Application, select Port Forwarding. Next select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the Rule Name, Protocol and Port number for your application.

For example, if you want to host a Netmeeting session, from the Home screen, click Advanced and under Application, select Port Forwarding. First select the IP address for your Netmeeting server. Next select the Audio/Video category and add Netmeeting to the applied rules box. To view the management rules, highlight Netmeeting and select view; this will display the pre configured protocols and ports that Netmeeting will use. Now assuming that your WAN connection is correct, you can run Netmeeting from your server and call users that are on the Internet. If you know your WAN IP address, users can call you. See Figure 1-33.



Port Forwarding

WAN Connection: quickstart ☐ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.2

Category

● Games
○ VPN
○ Audio/Video
○ Apps
○ Servers
○ User

Available Rules

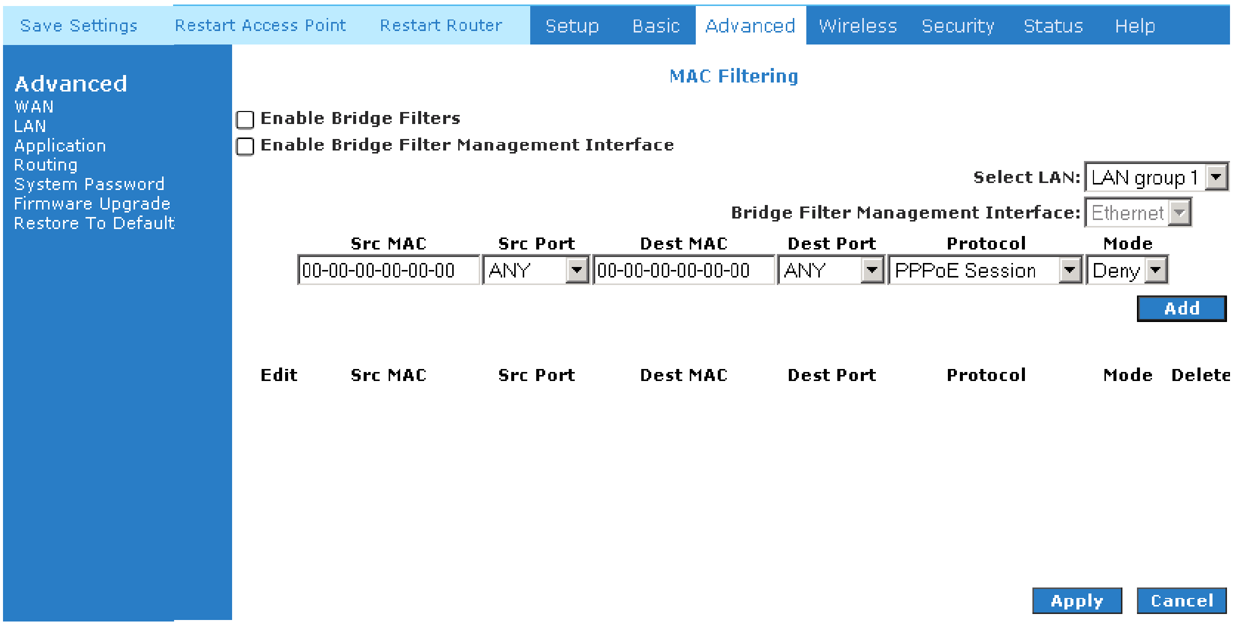
Alien vs Predator
Asheron's Call
Dark Rein 2
Delta Force
Doom
Dune 2000
DirectX (7,8) Games
EliteForce
EverQuest
Fighter Ace II

Applied Rules

Figure 1-33 : Port Forwarding

4.5.22 Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against each defined filter rules sequentially. When a match is determined, the appropriate filtering action (determined by the access type selected i.e. allow or deny) is performed. Please note that the bridge filter will only examine frames from interfaces, which are part of the bridge itself. Twenty filter rules are supported with bridge filtering. See Figure 1-34.



MAC Filtering

□ Enable Bridge Filters

□ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet

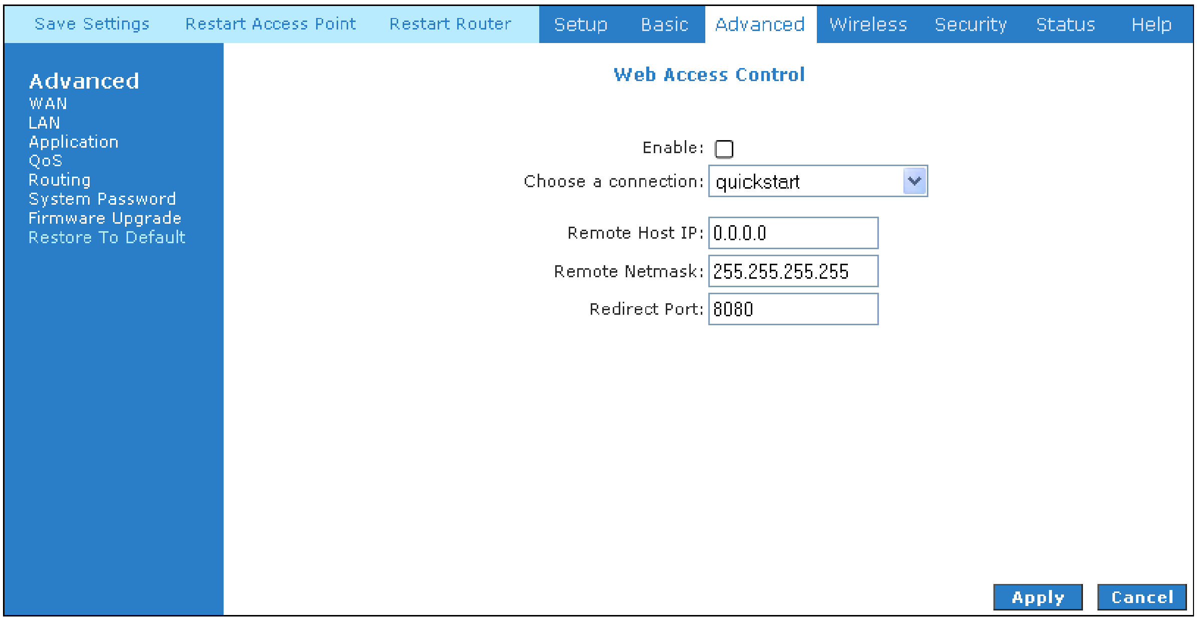
Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Figure 1-34 : MAC Filtering (Bridge Filters)

4.5.23 Web Access Control

The Web Access Control page allows you to access the router remotely via the web from the WAN side. See Figure 1-35.



Web Access Control

Enable: □

Choose a connection: quickstart

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

Redirect Port: 8080

Figure 1-35 : Web Access Control

If you want to access your router at home from a remote location such as your office, configure your WAN IP address using the following procedure.

4.5.23.1 Enable Web Access Control (WAN-Side)

1. Check Enable to enable the web access control feature.

2. In the Choose a connection field, select the connection used to connect to the Internet.

3. In the Remote Host IP field, enter the WAN-side IP address you will use to access your router (for example, 10.10.10.1).

4. In the Remote Netmask field, enter the netmask of your WAN-side IP address.

5. Enter a port number In the Redirect Port field (for example, 80).

6. Click Apply to temporarily activate the settings on the page.

This WAN address is added to the IP Access List. This allows you to access you router at home from a WAN IP (10.10.10.1) via Web.

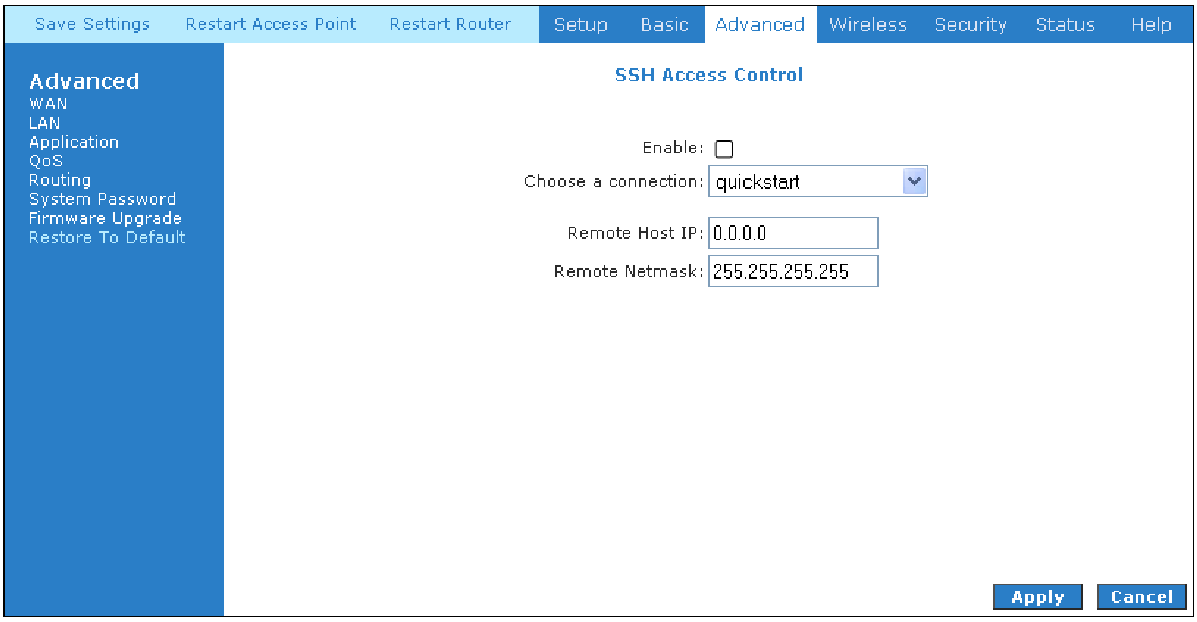
Note—The changes take effect when you click Apply; however, if the router configuration is not saved, these changes will be lost upon router reboot.

7. To access your router from the remote IP (10.10.10.1), enter the following in the

   URL: http(s)://WAN IP of router:Port Number

4.5.24 SSH Access Control

The SSH Access Control page allows you to access the router remotely via SSH from the WAN side. See Figure 1-36.



SSH Access Control

Enable: □

Choose a connection: quickstart

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

Figure 1-36 : SSH Access Control

4.5.24.1 Enable SSH Access Control (WAN-Side)

1. Check Enable to enable the SSH access control feature.
2. In the Choose a connection field, select the connection used to connect to the Internet.
3. In the Remote Host IP field, enter the WAN-side IP address you will use to access your router (for example, 10.10.10.1).
4. In the Remote Netmask field, enter the netmask of your WAN-side IP address.
5. Click Apply to temporarily activate the settings on the page.

   Note—The changes take effect when you click Apply; however, if the router configuration is not saved, these changes will be lost upon router reboot.

6. To access your router from the remote IP (10.10.10.1), enter the following in the

   URL: http(s)://WAN IP of router:Port Number

4.5.25 QoS

QoS stands for Quality of service. The QoS framework allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different QoS marking is used in different network:

• ToS network: ToS bits in the IP header

• VLAN network: priority bits in the VLAN header

• DSCP network: uses only 5 bits of the CoS

• WLAN: WLAN QoS header

The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the router has full control over packets from the time they enter the router till they leave the router. This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enter the router, and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the router.

There are 6 types of CoS (in descending priority):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

The rules are:

1. **CoS1** has absolute priority and is used for expedited forwarding (EF) traffic. This is always serviced till completion.

2. **CoS2-CoS5** are used for assured forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme:

CoS2 > **CoS3** > **CoS4** > **CoS5**

3. **CoS6** is for best effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your router, all traffic will be treated as best effort.

There are some additional terms you should get familiarize with:

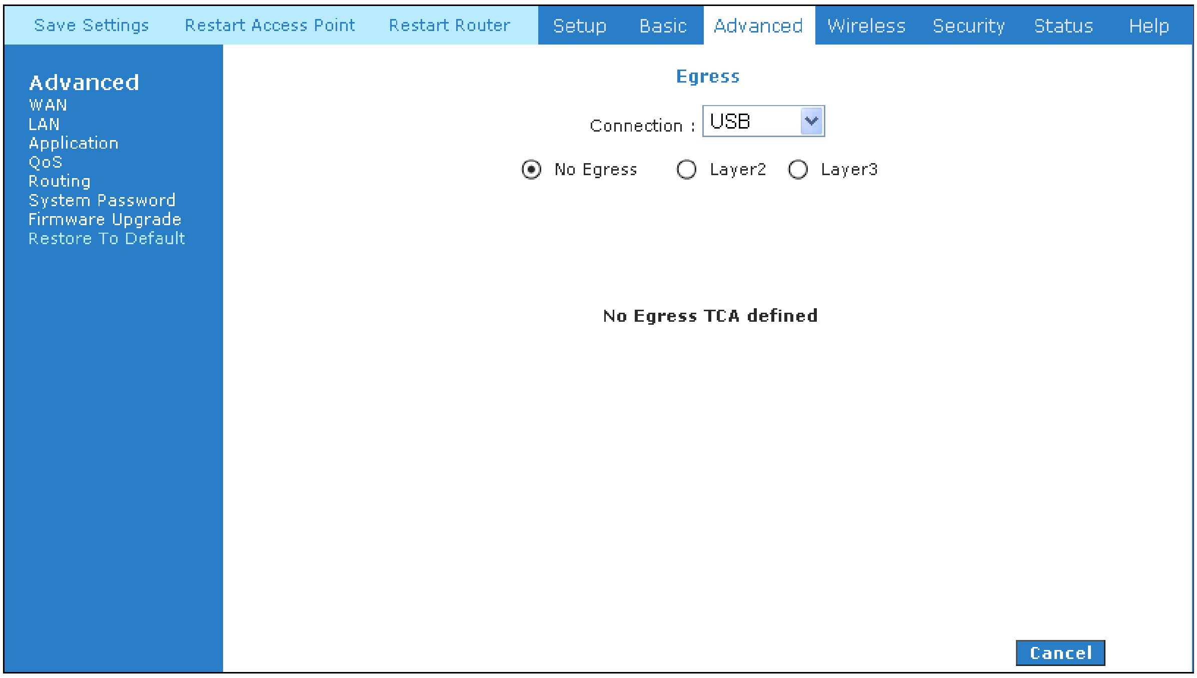
- Ingress: Packets arriving into the router from a WAN/LAN interface.
- Egress: Packets sent from the router to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:
  – Ingress mappings (Domain =>CoS)
  – Egress Mappings (CoS => Domain)
  – By default, all interfaces are in Untrusted mode.
- Shaper

4.5.26 Egress

For packets going out of the router, the marking (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the Egress page. This page is access by selecting Egress on the **Advanced** main page under **QoS**.

4.5.26.1 No Egress Mode

The default Egress page setting for all interfaces is No Egress. In this mode, the domain mappings of the packets are untouched.



Egress

Connection : USB

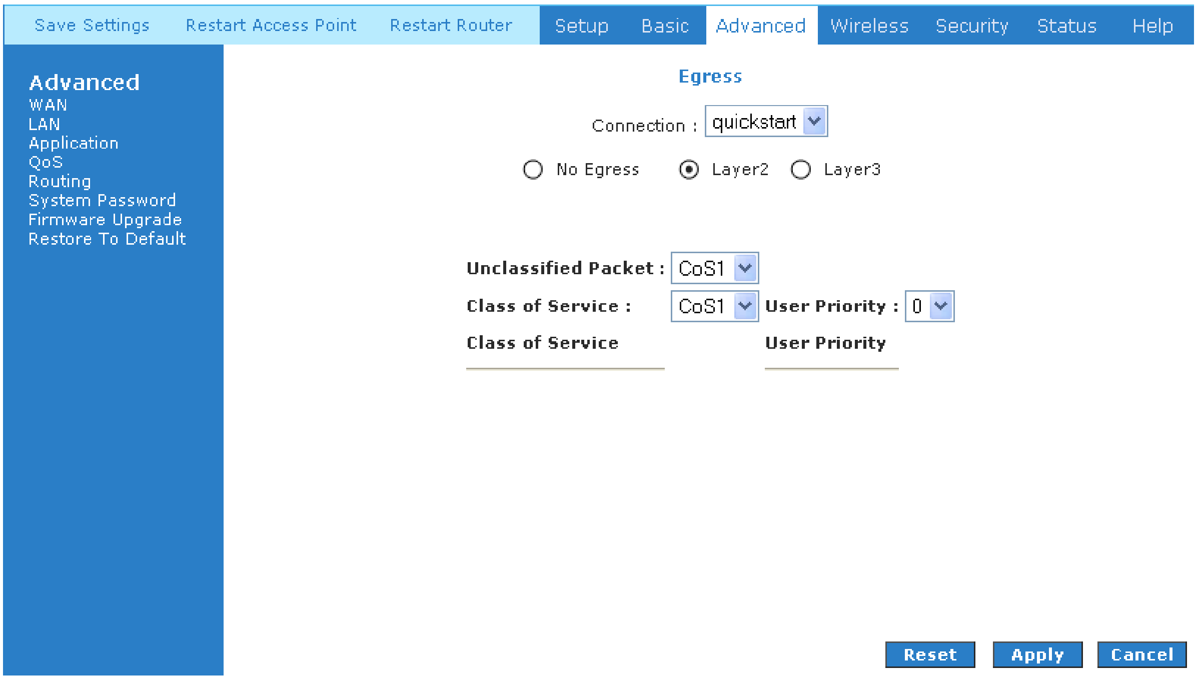
● No Egress ○ Layer2 ○ Layer3

No Egress TCA defined

Figure 1-37 : No Egress

4.5.26.2 Egress Layer 2 Configuration

The Egress Layer 2 page allows you to map the CoS of an outgoing packet to user priority bits, which is honoured by the VLAN network. Again, this feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current release.



Egress

Connection : quickstart

○ No Egress ● Layer2 ○ Layer3

Unclassified Packet : CoS1

Class of Service : CoS1 User Priority : 0

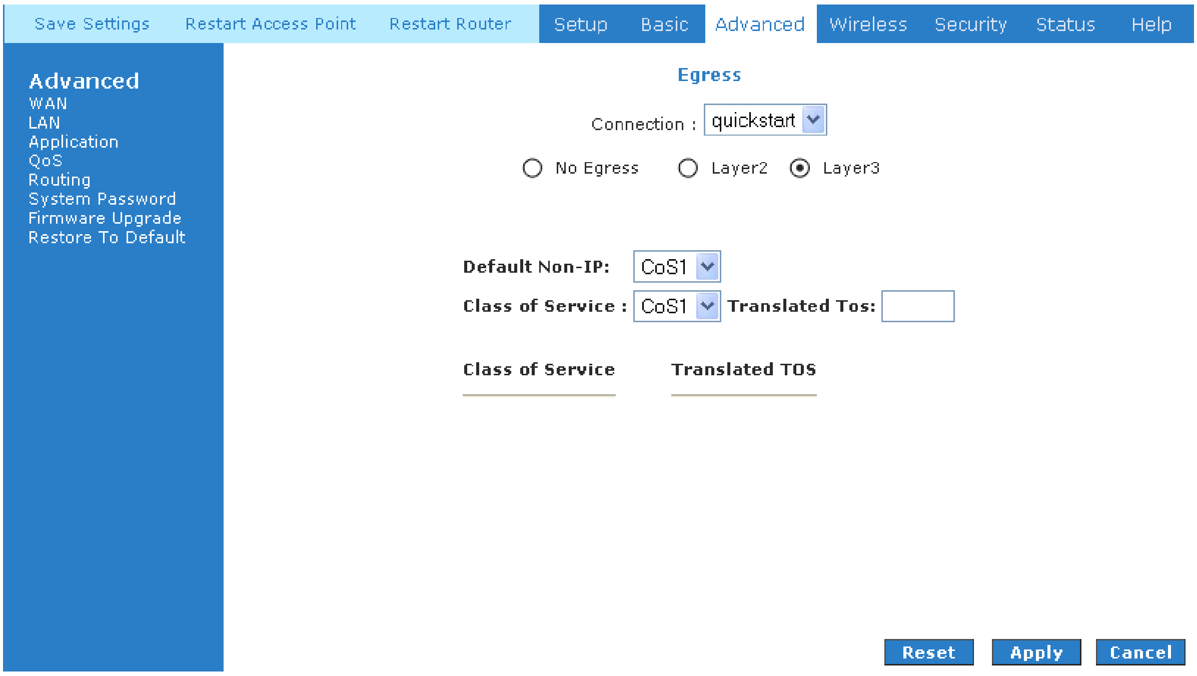
Class of Service User Priority

Figure 1-38 : Egress Layer 2

Field	Definition/ Description
Interface	Select the WAN interface to configure the QoS for outgoing packets, LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
Unclassified Packet	Some locally generated packets might not have been classified and thus do not have a CoS value, such as PPP control packet and ARP packet. You can define the CoS for all unclassified outgoing packets on layer 2 using this field, which will then pick up the user priority bits based on the mapping rules you create. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.

4.5.26.3 Egress Layer 3 Configuration

The Egress Layer 3 page enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.



Connection : quickstart

○ No Egress ○ Layer2 ● Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service	Translated TOS

Figure 1-39 : Egress Layer 3

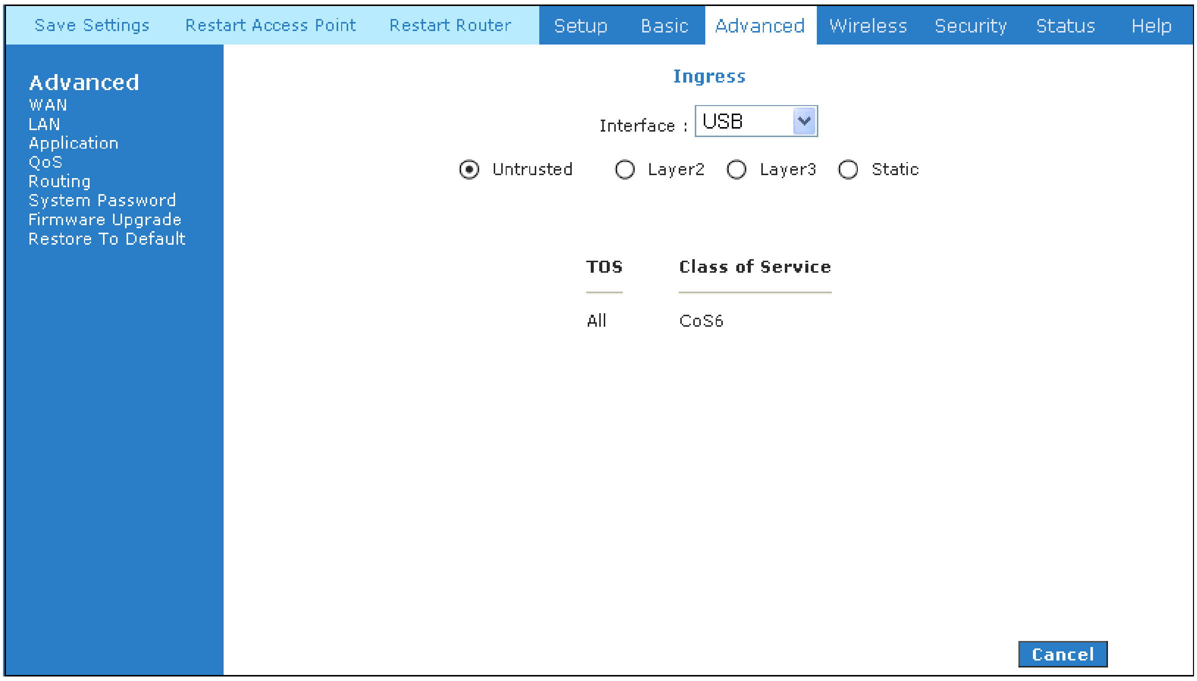
Field	Definition/ Description
Interface	Select the WAN/LAN interface here to configure the QoS for outgoing traffic to the IP network.
Default Non-IP	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
Translated ToS	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6, 7.

4.5.27 Ingress

The Ingress page enables you to configure QoS for packets as soon as they come into the router. This page is accessed by selecting Ingress on the **Advanced** main page under QoS**.** The domain mappings are converted to CoS (the common language) so that the priority marking is carried over. There are four modes that are discussed below:

4.5.27.1 Ingress Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honoured in the router. All packets are treated as CoS6 (best effort) as shown in Figure 1-40.



Ingress

Interface : USB

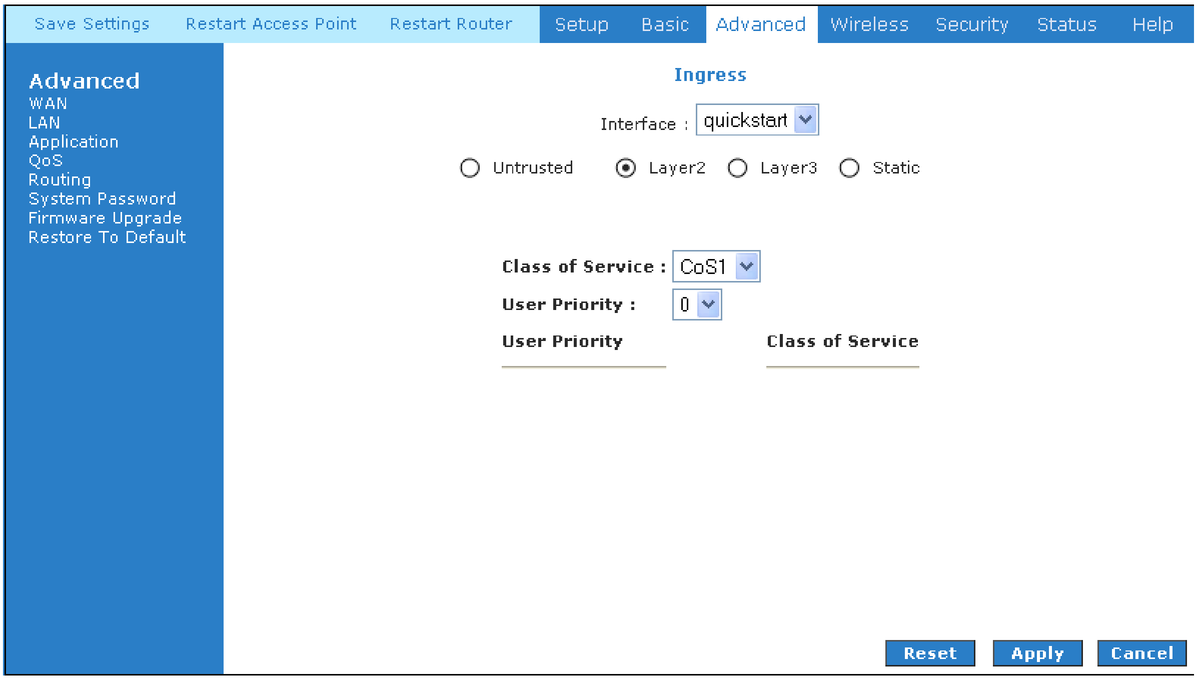
● Untrusted ○ Layer2 ○ Layer3 ○ Static

TOS	Class of Service
All	CoS6

Figure 1-40 : Ingress Untrusted Mode

4.5.27.2 Ingress Layer 2 Configuration

Layer 2 page allows you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.



Ingress

Interface : quickstart

○ Untrusted ● Layer2 ○ Layer3 ○ Static

Class of Service : CoS1

User Priority : 0

User Priority	Class of Service

Figure 1-41 : Ingress Layer 2 Configuration

Field	Definition/ Description
Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.

Ingress Layer 2 Priority Bits to CoS Configuration

1. From **Interface** drop-down box, select *quickstart*.

   You are configuring QoS on this WAN interface.

2. Select *CoS1* in **Class of Service** and 5 in **Priority Bits**.

   Any packets with priority marking 5 is mapped to *CoS1*, the highest priority that is normally given to the voice packets.

3. Click **Apply** to temporarily activate the settings.

4. Select *CoS2* in the **Class of Service** field and *1* in the **Priority Bits** field. Any packets that have a priority bits of *1* is mapped to *CoS2*, which is the second highest priority. This is given to the high priority packets such as video.

5. Click **Apply** to temporarily activate the settings.

   Note—The changes take effect when you click **Apply**; however, if the router configuration is not saved, these changes will be lost upon reboot.

6. Repeat step 2-5 to add more rules to *quickstart*.

   Up to eight rules can be configured for each interface.

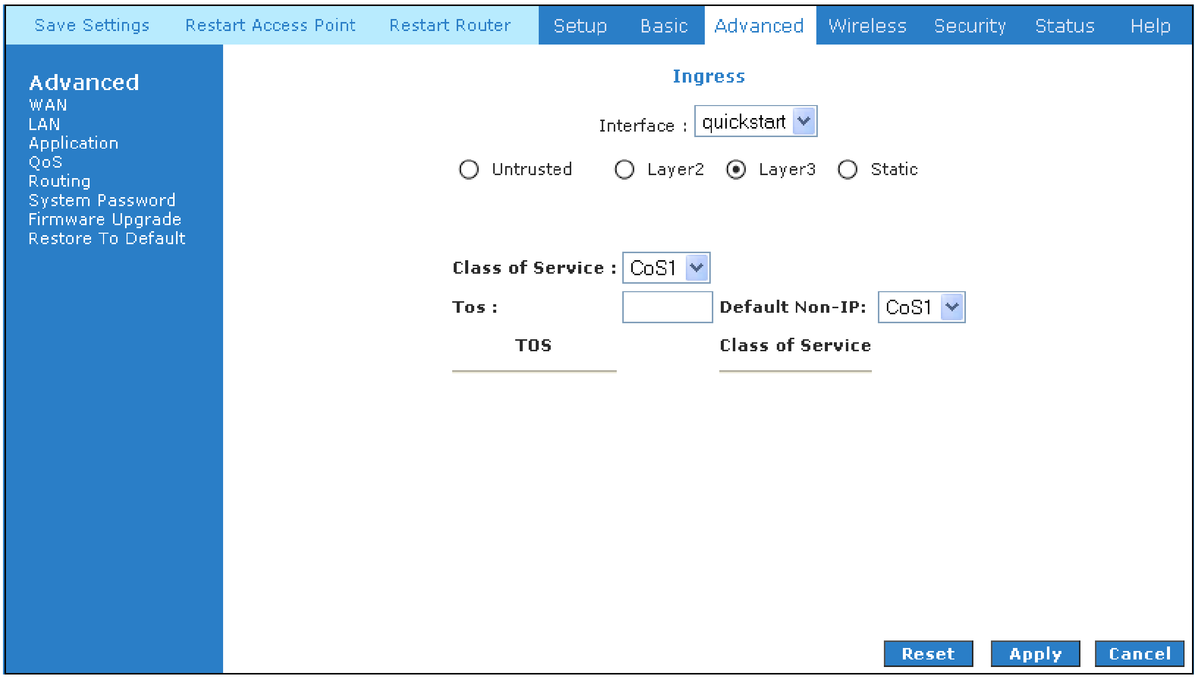
   Note—Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority.

7. Repeat step 1-6 to create rules to another WAN interface.

   Note—Any WAN interface that is not configured has the default *Untrusted* mode.

4.5.27.3 Ingress Layer 3 Configuration

The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.



Ingress

Interface : quickstart

○ Untrusted ○ Layer2 ● Layer3 ○ Static

Class of Service : CoS1

Tos : Default Non-IP: CoS1

TOS Class of Service

Figure 1-42 : Ingress Layer 3 Configuration

Field	Definition/ Description
Interface	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
Class of Service	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
ToS	The Type of Service field takes values from 0 to 255.
Default Non-IP	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have an IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).

Ingress Layer 3 ToS to CoS Configuration

1. From Interface drop-down box, select *LAN Group 1*.

   You are configuring QoS on this interface.

2. Select *CoS1* in Class of Service and enter *22* in Type of Service (ToS).

   Any incoming packet from LAN Group 1 (layer 3) with a ToS of *22* is mapped to *CoS1*, the highest priority, which is normally given to the voice packets.

3. Leave the default value *CoS1* in Default Non-IP.

   Any incoming packet from LAN Group 1 without an IP is mapped to CoS1, the highest priority.

4. Click Apply to temporarily activate the settings.

   Note—The changes take effect when you click Apply; however, if the router configuration is not saved, these changes will be lost upon reboot.

5. Repeat step 2-4 to add more rules to LAN Group 1.

   Up to 255 rules can be configured for each interface.

   Note—Any ToS that have not been mapped to a CoS is treated as CoS6, the lowest priority.

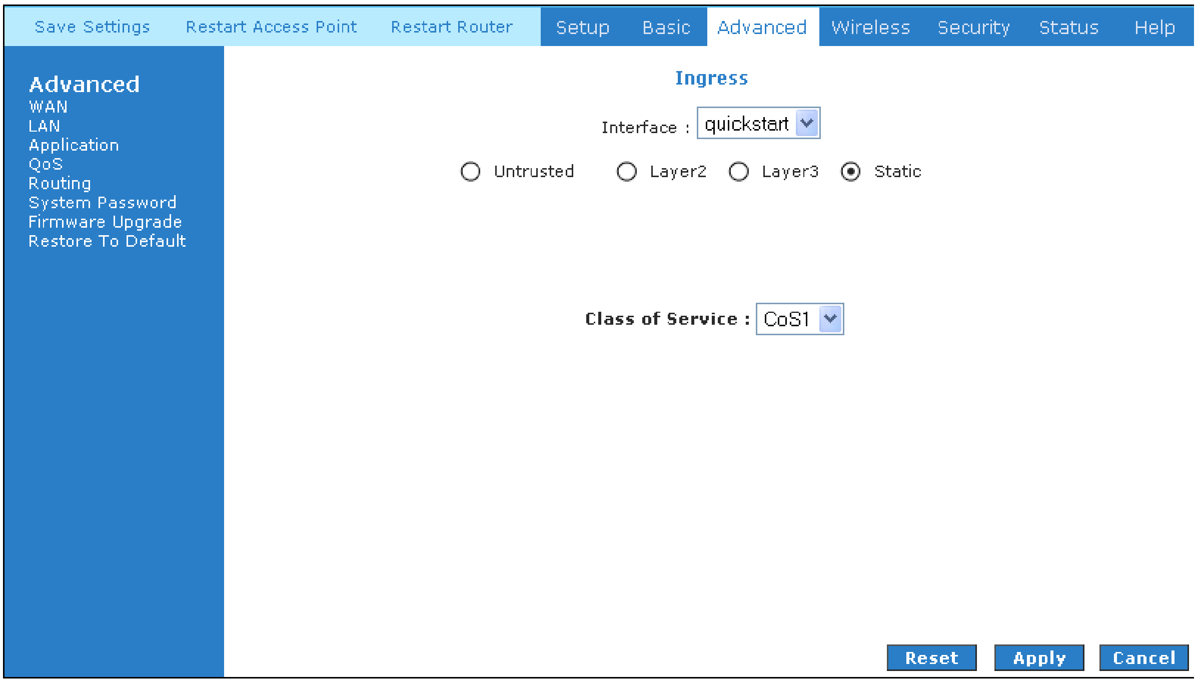
6. Repeat step 1-5 to create rules to another WAN/LAN interface.

   Note—Any WAN/LAN interface that is not configured has the default *Untrusted* mode.

7. To make the change permanent, click Save Settings.

4.5.27.4 Ingress Static Configuration

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.



Ingress

Interface : quickstart

○ Untrusted ○ Layer2 ○ Layer3 ● Static

Class of Service : CoS1

Figure 1-43 : Ingress Static Configuration

To configure, follow the following procedure to configure Ingress static QoS settings.

Ingress Static Configuration

1. At the Interface drop-down box, select *USB*.

   You are configuring QoS on this interface only. Any WAN/LAN interface that isnot configured has the default *Untrusted* mode.

2. Select *CoS1* in Class of Service.

   All incoming traffic from the USB interface receives CoS1, the highest priority.

3. Click Apply to temporarily activate the settings.

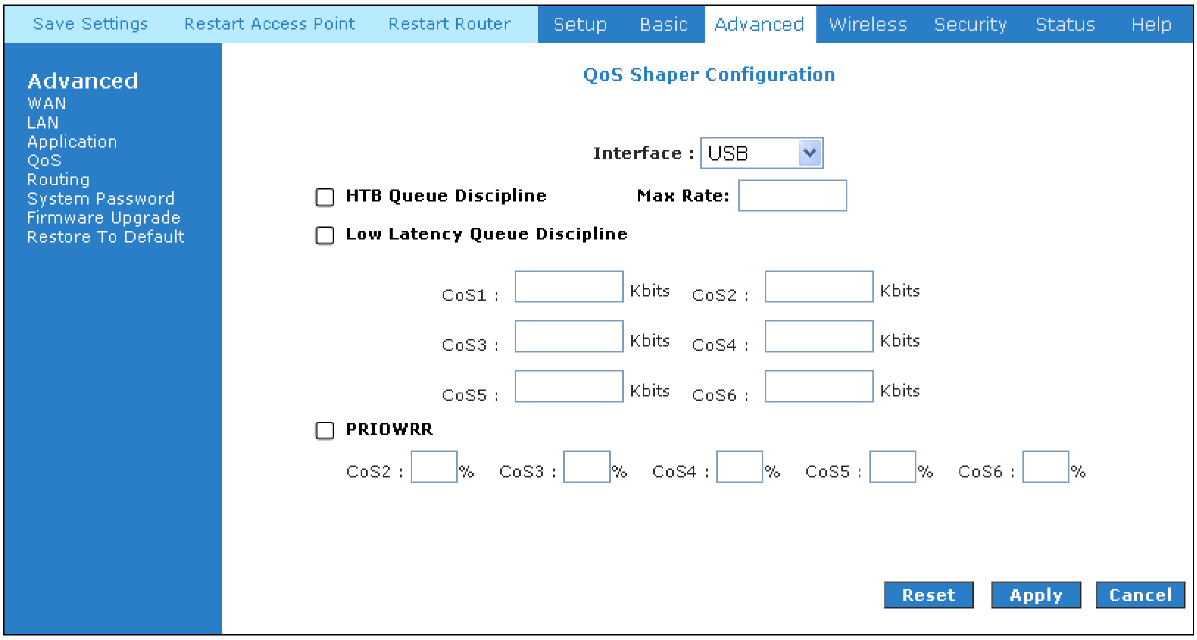
   Note—The changes take effect when you click Apply; however, if the router configuration is not saved, these changes will be lost upon reboot.

4.5.28 QoS Shaper Configuration

The **Shaper Configuration** page is accessed by selecting **Shaper** on the **Advanced** main page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR

Note—Egress TCA is required if shaper is configured for that interface.



QoS Shaper Configuration

Interface : USB

☐ HTB Queue Discipline Max Rate:

☐ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

☐ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Figure 1-44 : QoS Shaper Configuration

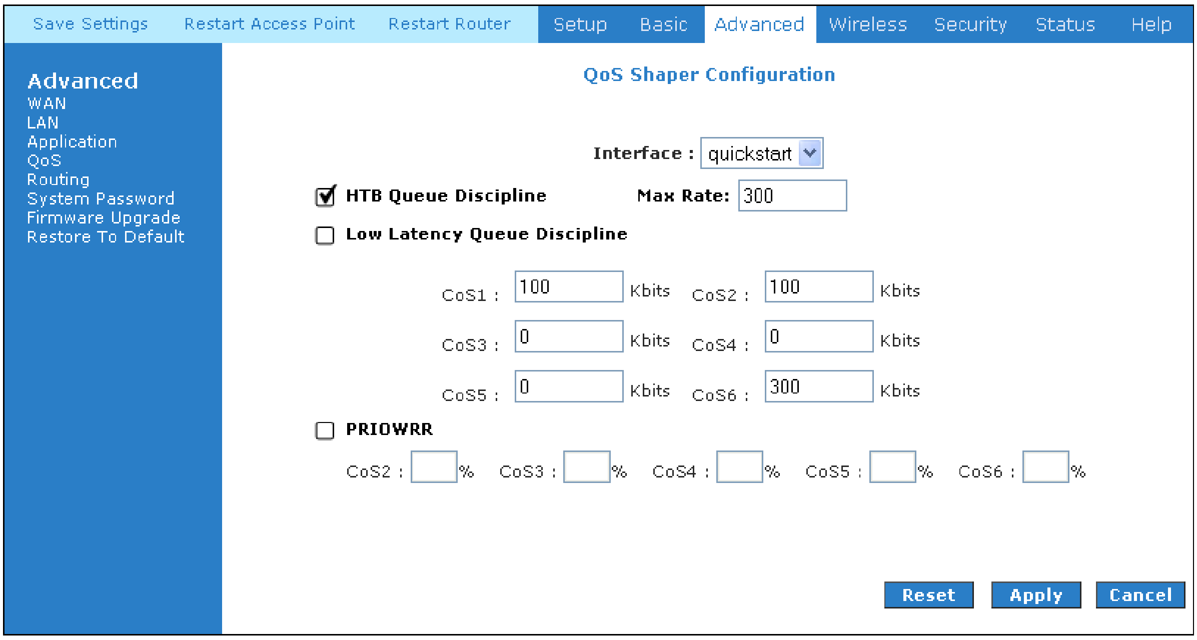
Field	Definition/ Description
Interface	The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.
Max Rate	This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline, both are rate-based shaping algorithms.
HTB Queue Discipline	The hierachical token bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic is assigned a specific rate to which data will be shaped to. For example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.
Low Latency Queue	This is similar to the above algorithm except that CoS1 is not rate

Discipline	limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.
PRIOWRR	This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.

Of the three shaping algorithms available on the **Shaper Configuration** page, only one can be enabled at a time. An example of each configuration is given as follows.

Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300 kbits of bandwith, of which 100 kbits is given to CoS1 and another 100 kbits is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 kbits of bandwith.



QoS Shaper Configuration

Interface : quickstart

☑ HTB Queue Discipline Max Rate: 300

□ Low Latency Queue Discipline

CoS1 : 100 Kbits CoS2 : 100 Kbits

CoS3 : 0 Kbits CoS4 : 0 Kbits

CoS5 : 0 Kbits CoS6 : 300 Kbits

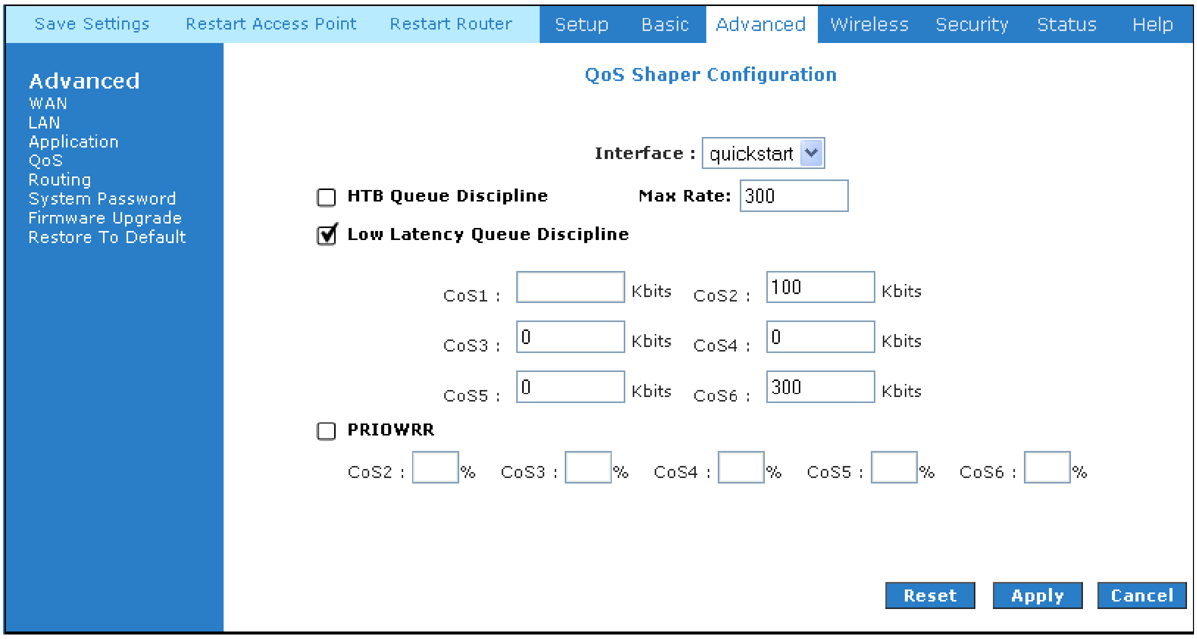
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Figure 1-45 : HTB Queue Discipline enabled

Example 2: Low Latency Queue Discipline Enabled

In this second example, Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 kbits when there is no CoS1 packets. CoS6 has 300 kbits when there is no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.



QoS Shaper Configuration

Interface : quickstart

□ HTB Queue Discipline Max Rate: 300

☑ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : 100 Kbits

CoS3 : 0 Kbits CoS4 : 0 Kbits

CoS5 : 0 Kbits CoS6 : 300 Kbits

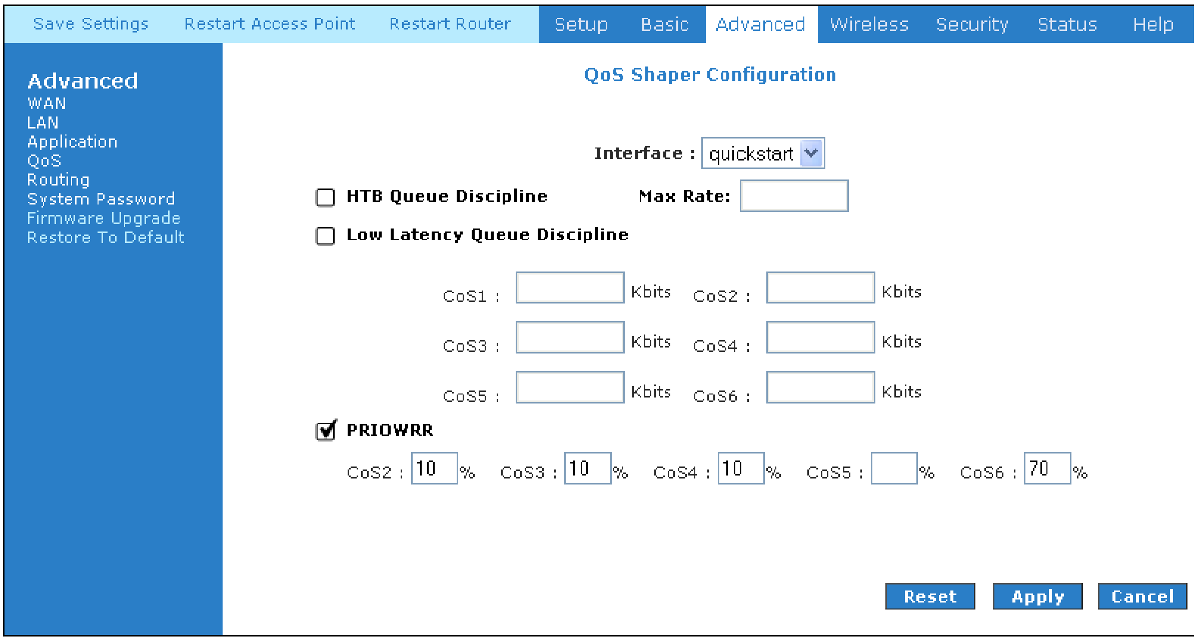
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Figure 1-46 : Low Latency Queue Discipline enabled

Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there is no CoS1 packets, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the Low Latency Queue discipline, except that one is packet-based, and the other is rate-based.



QoS Shaper Configuration

Interface : quickstart

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

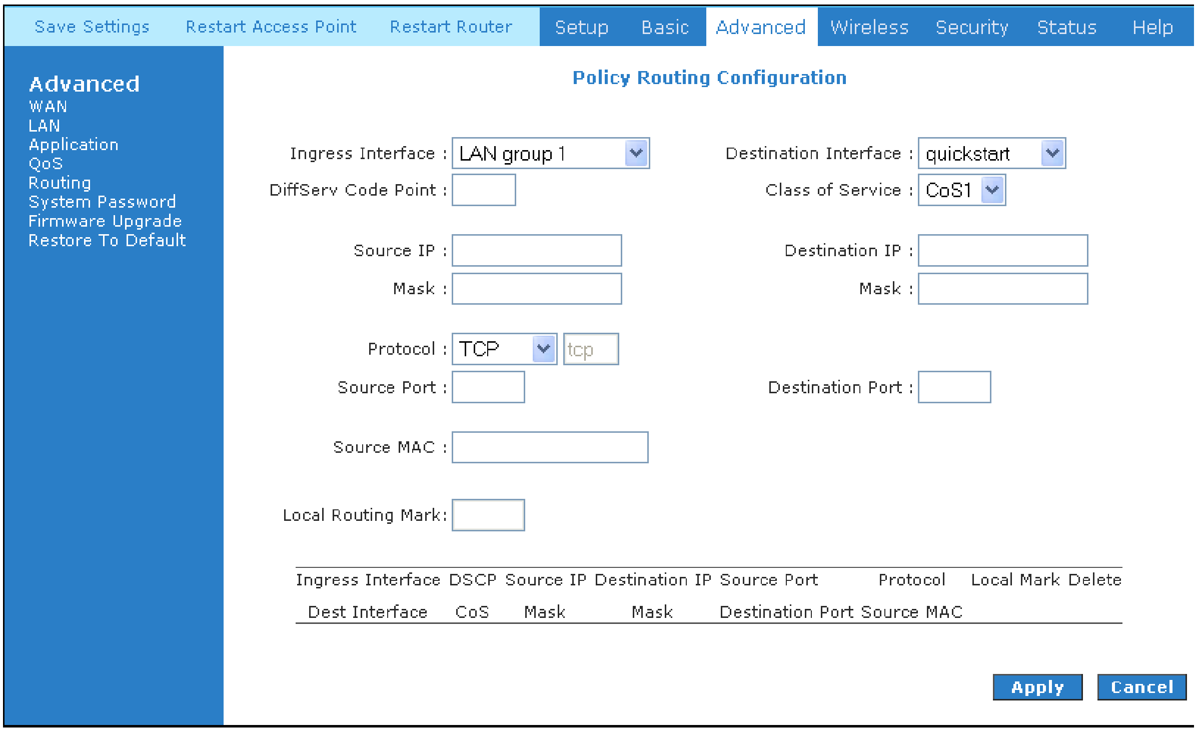
☑ PRIOWRR

CoS2 : 10 % CoS3 : 10 % CoS4 : 10 % CoS5 : % CoS6 : 70 %

Figure 1-47 : PRIOWRR enabled

4.5.29 Policy Routing Configuration

The Policy Routing Configuration page is accessed by selecting Policy Routing Configuration on the Advanced home page under QoS. This page enables you to configure policy routing and QoS. The policy routing configuration is discussed as follows. The QoS configuration is discussed in ‘‘Ingress Payload Database Configuration’’.



Policy Routing Configuration

Ingress Interface : LAN group 1

Destination Interface : quickstart

DiffServ Code Point :

Class of Service : CoS1

Source IP :

Destination IP :

Mask :

Mask :

Protocol : TCP tcp

Source Port :

Destination Port :

Source MAC :

Local Routing Mark:

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete
Dest Interface	CoS	Mask	Mask	Destination Port	Source MAC		

Figure 1-48 : Policy Routing Configuration

Field	Definition/ Description
Ingress Interface	The incoming traffic interface for a Policy Routing rule. Selections include *LAN interfaces*, *WAN interfaces*, *Locally generated (traffic)*, and *not applicable*. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.
Destination Interface	The outgoing traffic interfaces for a Policy Routing rule. Selections include *LAN Interfaces* and *WAN interfaces*.
DiffServ Code Point	The diffServ code point (DSCP) field value ranges from *1 to 255*. This field cannot be configured alone, addtional fields like IP, Source MAC, and/or Ingress Interface should be configured.
Class of Service	The selections are (in the order of priority): *CoS1*, *CoS2*, *CoS3*, *CoS4*, *CoS5*, *CoS6*, and *N/A*.
Source IP	The IP address of the traffic source.
Mask	The source IP netmask. This field is required if the source IP has

	been entered.
Destination IP	The IP address of the traffic destination.
Mask	The netmask of the destination. This field is required if the destination IP has been entered.
Protocol	The selections are *TCP*, *UDP*, *ICMP*, *Specify*, and *none*. If you choose *Specify*, you need to enter the protocol number in the box next to the **Protocol** field. This field cannot be configured alone, addtional fields like **IP**, **Source MAC**, and/or **Ingress Interface** should be configured. This field is also required if the source port or destination port has been entered.
Source Port	The source protocol port. You cannot configure this field without entering the protocol first.
Destination Port	The destination protocol port or port range. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing MAC	This field is enabled only when *Locally Generated* is selected in the **Ingress Interface** field. The mark for DNS traffic generated by different applications are described below: • Dynamic DNS: 0xE1 • Dynamic Proxy: 0xE2 • Web Server: 0xE3 • MSNTP: 0xE4 • DHCP Server: 0xE5 • IPtables Utility: 0xE6 • PPP Deamon: 0xE7 • IP Route: 0xE8 • ATM Library: 0xE9 • NET Tools: 0xEA • RIP: 0xEB • RIP v2: 0xEC • UPNP: 0xEE

	• Busybox Utility: 0xEF • Configuration Manager: 0xF0 • DropBear Utility: 0xF1 • Voice: 0

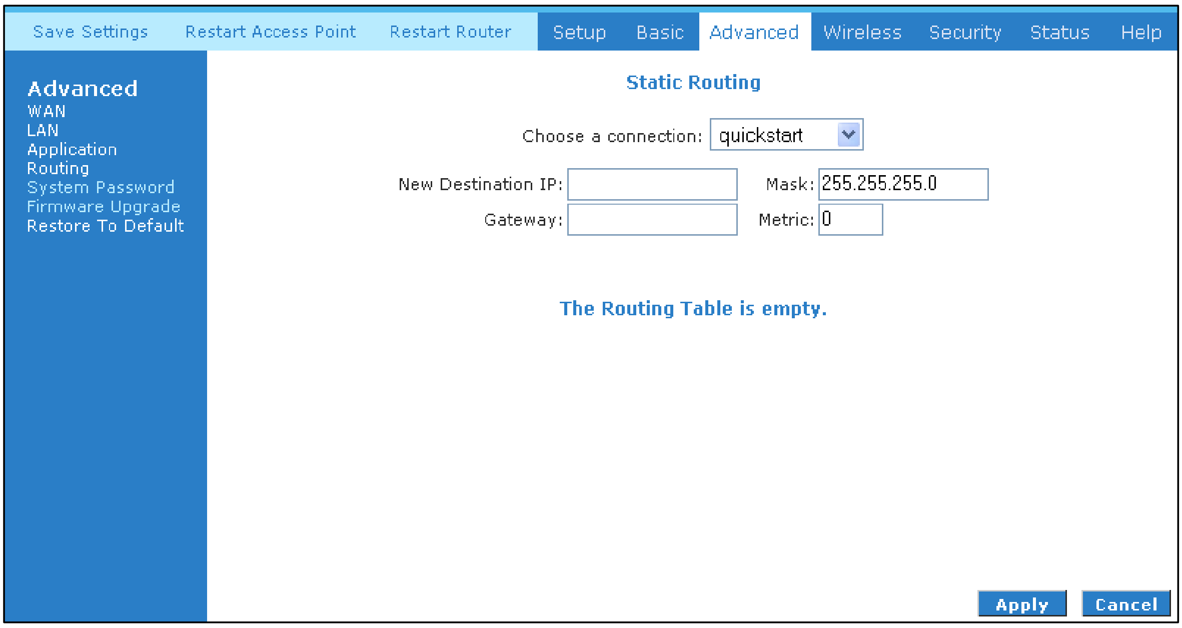
Currently routing algorithms make decision based on destination address, i.e. only Destination IP address and subnet mask is supported. The **Policy Routing** page enables you to route packets on the basis of various fields in the packet. The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

4.5.30 Static Routing

If the ADSL Router is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the ADSL Router.

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. See Figure 1-49.



Static Routing

Choose a connection: quickstart

New Destination IP: Mask: 255.255.255.0

Gateway: Metric: 0

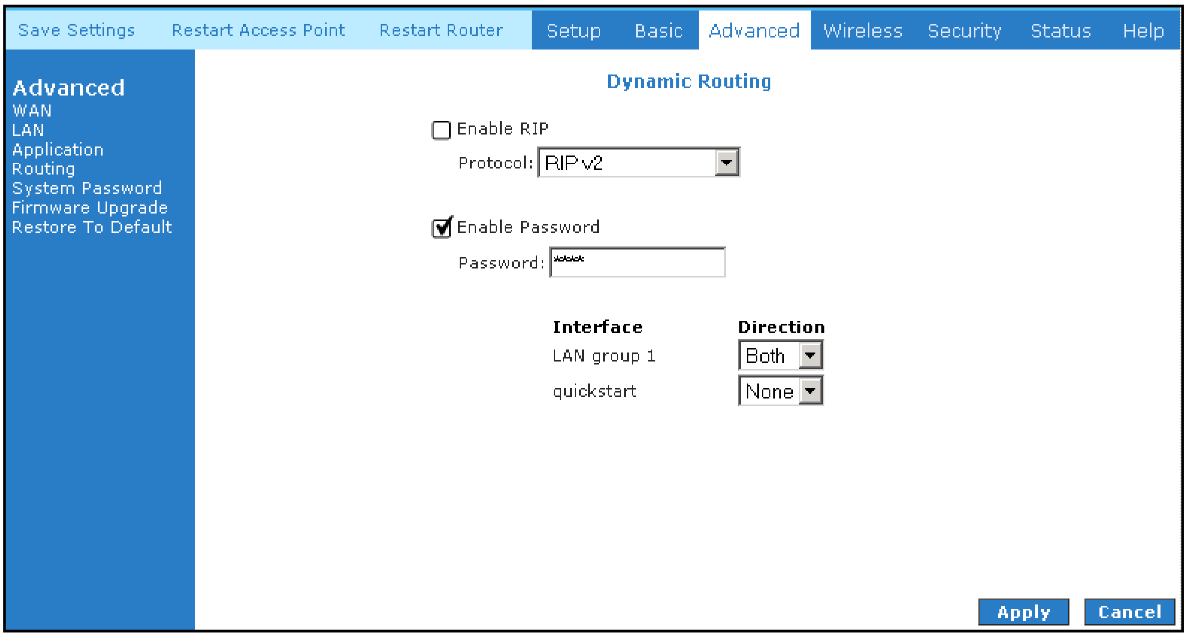
The Routing Table is empty.

Figure 1-49 : Static Routing

4.5.31 Dynamic Routing

Dynamic Routing allows the ADSL Router to automatically adjust to physical changes in the network. The ADSL Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other ADSL Routers on the network. The Direction determines the direction that RIP routes will be updated. Selecting **In** means that the ADSL Router will only incorporate received RIP information. Selecting **Out** means that the ADSL Router will only send out RIP information. Selecting **Both** means that the ADSL Router will incorporate received RIP information and send out updated RIP information.

The protocol is dependent upon the entire network. Most networks support RIP v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If RIP v2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If RIP v1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting. See Figure 1-50.



Dynamic Routing

□ Enable RIP

Protocol: RIP v2

☑ Enable Password

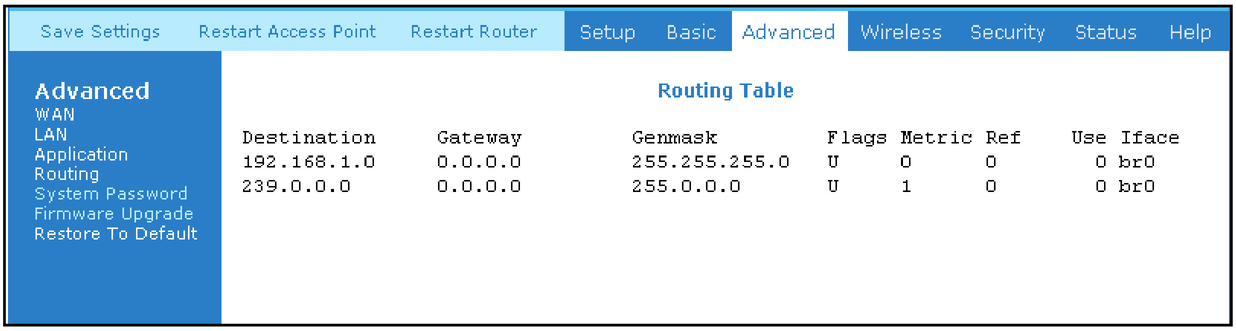
Password: ****

Interface	Direction
LAN group 1	Both
quickstart	None

Figure 1-50 : Dynamic Routing

4.5.32 Routing Table

Routing Table shows the information used by routers when making packet forwarding decisions. Packets are routed according to the packet's destination IP address. See Figure 1-51.



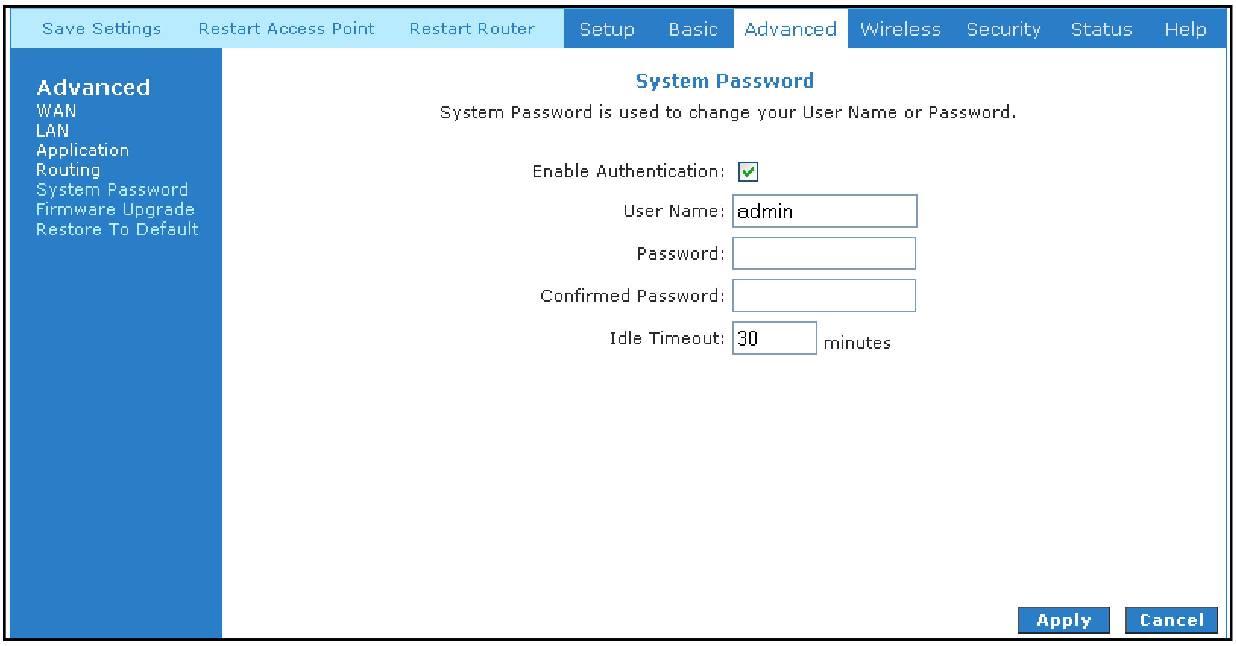
Routing Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 br0
239.0.0.0       0.0.0.0         255.0.0.0       U     1      0        0 br0
```

Figure 1-51 : Routing Table

4.5.33 System Password

You can change your ADSL Router's username and password by clicking on System Password. You can also change the idle timeout; you will need to log back onto the ADSL Router once the timeout expires. If you forget your password, you can press and hold the reset to factory defaults button for 10 seconds (or more). The ADSL Router will reset to its factory default configuration and all custom configurations will be lost. See Figure 1-52.



System Password

System Password is used to change your User Name or Password.

Enable Authentication: ☑

User Name: admin

Password:

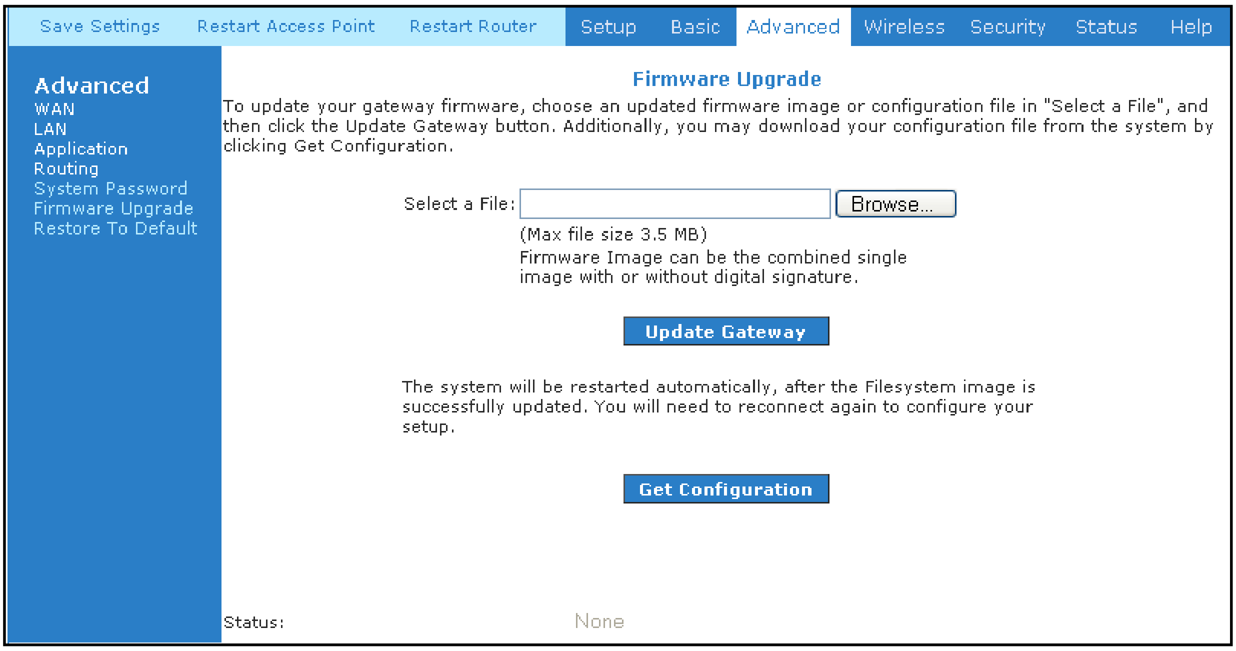
Confirmed Password:

Idle Timeout: 30 minutes

Figure 1-52 : System Password

4.5.34 Firmware Upgrade

You can upgrade the ADSL Router's firmware; click on Firmware Upgrade. To upgrade the firmware, click browse, find the firmware file to download. Make sure this is the correct file. Click on Update Gateway. Once the upgrade is complete the ADSL Router will reboot. You will need to log back onto the ADSL Router after the firmware upgrade is completed. The firmware upgrade should take about 5 minutes to complete. Note: Do not remove power from the ADSL Router during the firmware upgrade procedure. See Figure 1-53.



Firmware Upgrade

To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.

Select a File:

(Max file size 3.5 MB)
Firmware Image can be the combined single image with or without digital signature.

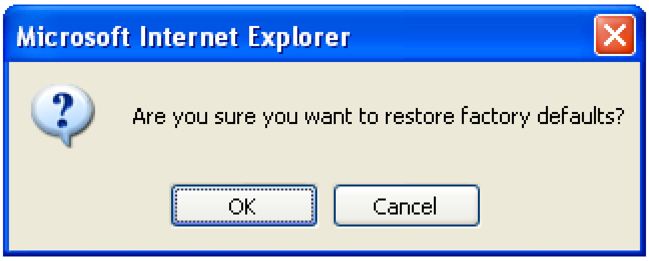
The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.

Status: None

Figure 1-53 : Firmware Upgrade

4.5.35 Restore to Default

The restore to factory defaults feature will set the ADSL Router to its factory default configuration by resetting the ADSL Router. A prompt as the one shown in Figure 1-54 will pop-up. You may need to reset the ADSL Router to its factory default if you lose the ability to interface ADSL Router via the web interface (or following a software upgrade). To reset the ADSL Router, simply press the reset button for ~10 seconds (or more). After about 30 ~ 40 seconds the ADSL Router will be operational again.



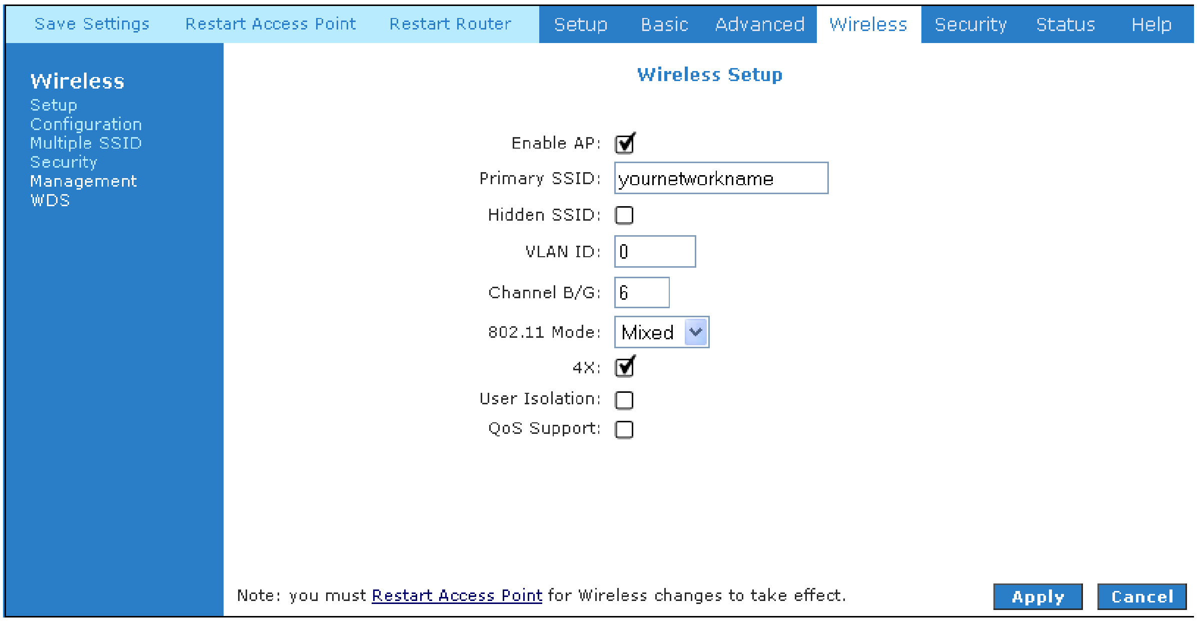
Are you sure you want to restore factory defaults?

Figure 1-54 : Restore to Default prompt

4.6 Wireless

4.6.1 Wireless Setup

The SSID default which is set as "yournetworkname" by default. It can be changed. SSID is wireless network name for the wireless router. Your wireless client will need this name for wireless connection. The wireless setup allows the user to enable or disable the AP (access point for the wireless feature). Disabling AP will prevent the wireless router from emitting any wireless signal. See Figure 1-55.



Wireless Setup

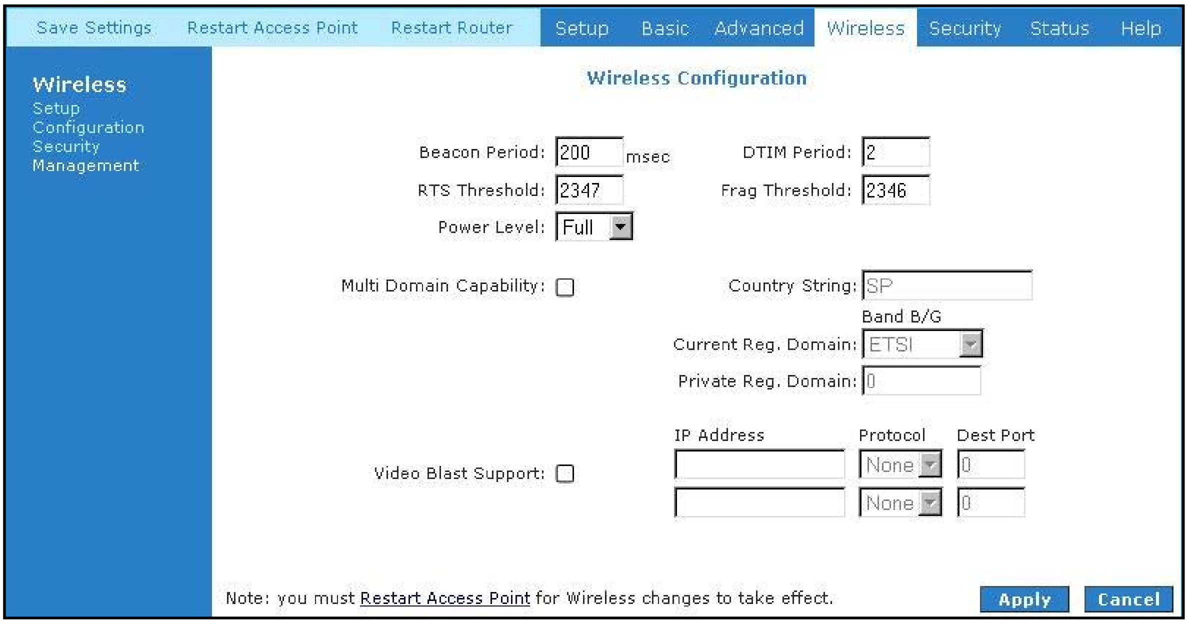
Enable AP: ☑
Primary SSID: yournetworkname
Hidden SSID: □
VLAN ID: 0
Channel B/G: 6
802.11 Mode: Mixed
4X: ☑
User Isolation: □
QoS Support: □

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-55 : Wireless Setup Page

4.6.2 Wireless Configuration

For users who want to explore the advanced features, you can click on the Advanced button. The options listed can be changed to cater for advance users. See Figure 1-56.



Wireless Configuration

Beacon Period: 200 msec   DTIM Period: 2

RTS Threshold: 2347   Frag Threshold: 2346

Power Level: Full

Multi Domain Capability: □   Country String: SP

Band B/G

Current Reg. Domain: ETSI

Private Reg. Domain: 0

IP Address	Protocol	Dest Port
	None	0
	None	0

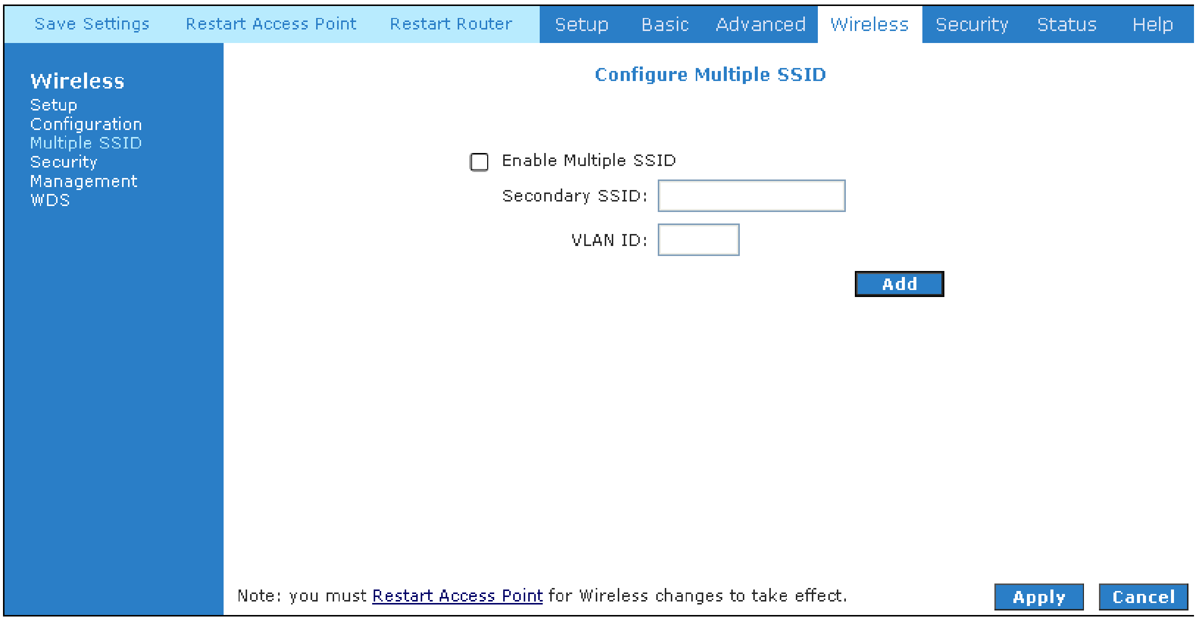
Video Blast Support: □

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-56 : Wireless Configuration Page

4.6.3 Multiple SSID

You can access the Multiple SSID page by clicking the Multiple SSID link. The **Enable Multple SSID** field allows you to create multiple SSIDs for the AP. The Multiple SSID feature supports up to two SSID (one primary and one secondary). The SSID field takes up to 32 alpha-numeric characters. Change the **VLAN ID** to a number different from zero (between 1 to 4095). Up to 3 secondary SSIDs are supported in addition to the primary SSID.



Configure Multiple SSID

□ Enable Multiple SSID

Secondary SSID:

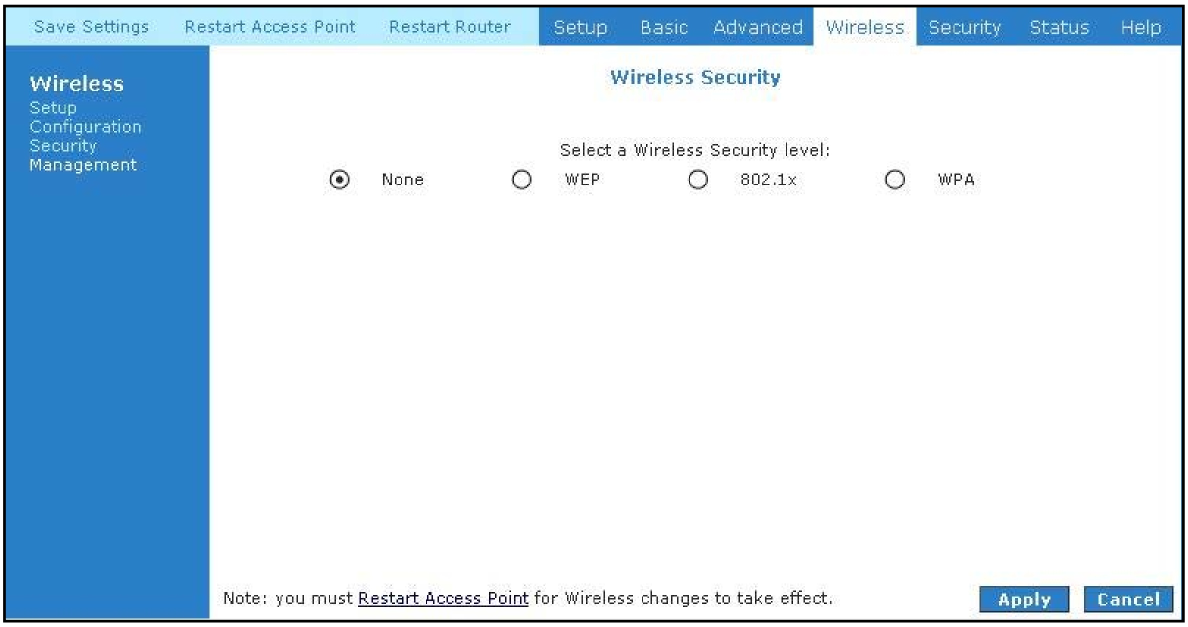
VLAN ID:

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-57 : Multiple SSID

4.6.4 Wireless Security

It is important for user to enforce security in wireless LAN environment. This is to prevent unauthorized wireless users from accessing your router. By default, the ‘None’ radio button is selected. See Figure 1-58.



Wireless Security

Select a Wireless Security level:

● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-58 : Wireless Security

4.6.4.1 WEP

WEP is a security protocol for WLAN. WEP provides security by encrypting the data that is sent over the WLAN.

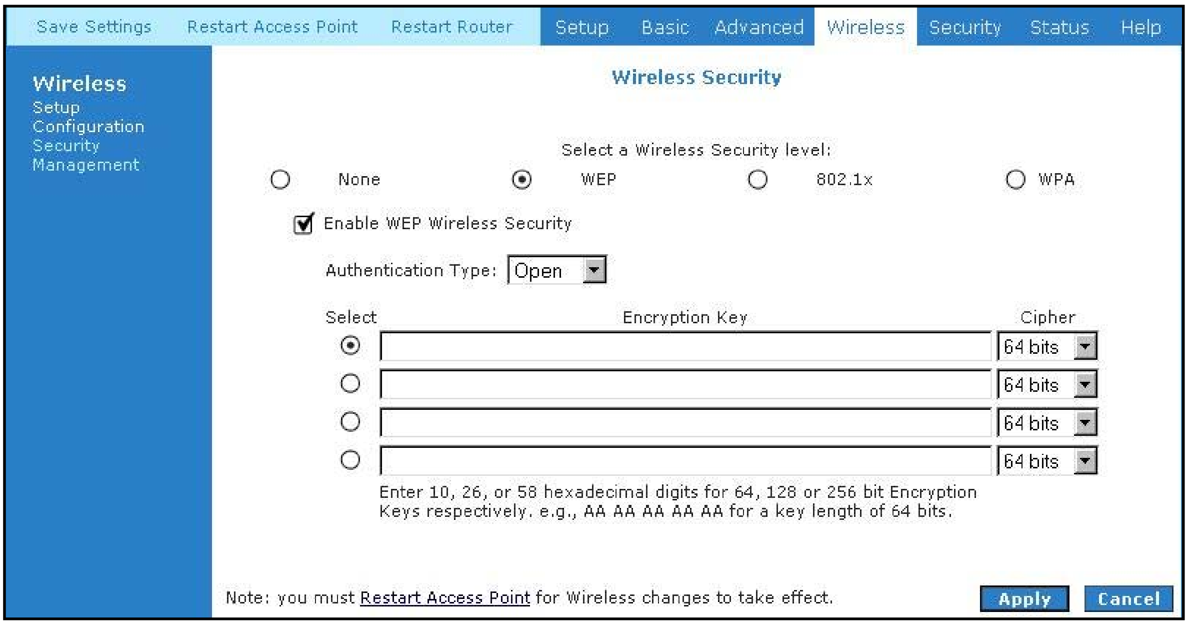
The router supports three levels of WEP encryption:

- 64-bit encryption
- 128-bit encryption
- 256-bit encryption

With WEP, the receiving station must use the same key for decryption. Each radio network interface card (NIC) and AP, therefore must be manually configured with the same key.

In order to implement security, proceed with the following steps. See Figure 1-59.

1. Select the WEP option.
2. Check on “Enable WEP Wireless Security” option.
3. Select the “Cipher”option, the available options are 64 bits, 128 bits and 256 bits.
4. You can configure up to 4 sets of keys for your wireless client.



Wireless Security

Select a Wireless Security level:

○ None ● WEP ○ 802.1x ○ WPA

☑ Enable WEP Wireless Security

Authentication Type: Open

Select	Encryption Key	Cipher
●		64 bits
○		64 bits
○		64 bits
○		64 bits

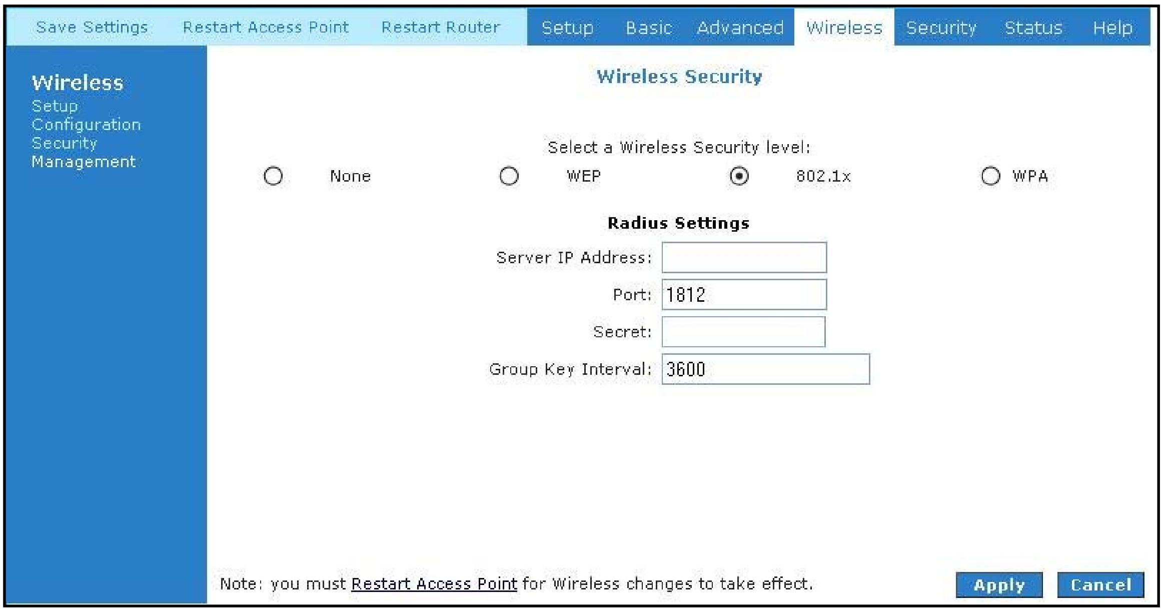
Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-59 : Wireless Security – WEP

4.6.4.2 802.1x

802.1x is a security protocol for WLAN. It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on extensible authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the remote authentication dial-in user service (RADIUS) protocol. Refer to **Error! Reference source not found.**. Enter the IP Address of the RADIUS Server (for 802.1x authentication purposes). This is used only when you have a RADIUS Server and want to use it for authentication. Almost all homes and offices do not have a RADIUS Server. Refer to Figure 1-60.



Wireless Security

Select a Wireless Security level:

○ None ○ WEP ● 802.1x ○ WPA

Radius Settings

Server IP Address:

Port: 1812

Secret:

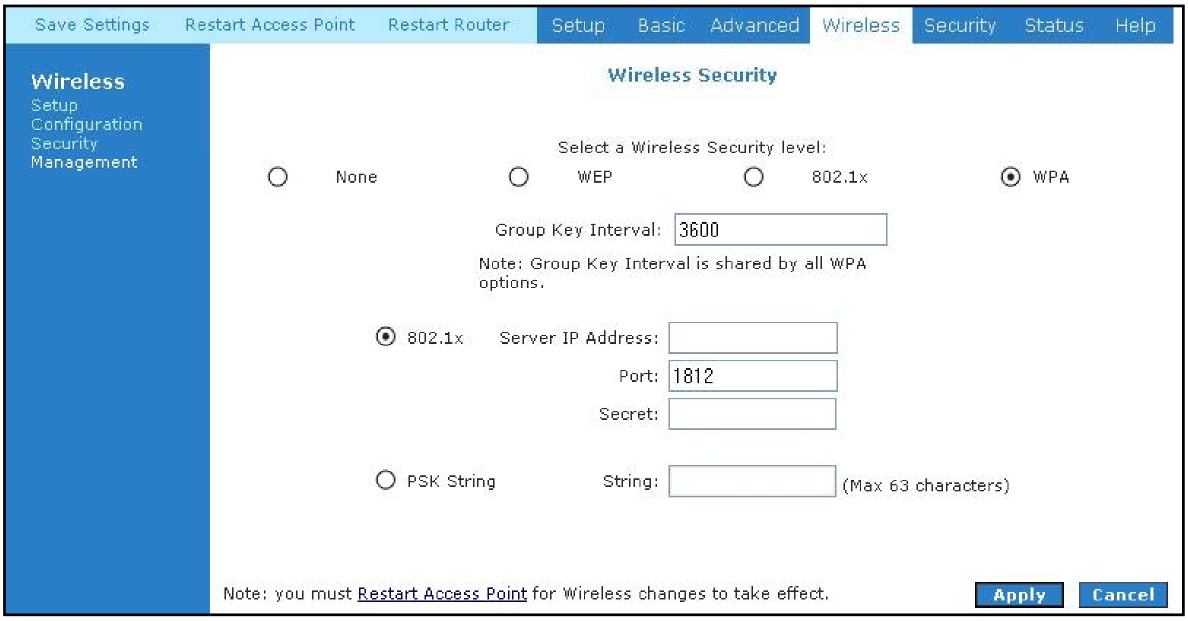
Group Key Interval: 3600

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-60 : Wireless Security – 802.1x

4.6.4.3 WPA

WPA is the short term for WiFi Protected Access. WPA is an industry-supported, pre-standard version of 802.11i that utilizes the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, which includes using dynamic keys. WPA uses a sophiscated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an AP. Protocols including 802.1X, EAP, and RADIUS are used for strong authentication. Like WEP, keys can still be entered manually (pre-shared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. WPA uses temporal key integrity protocol (TKIP) for data encryption. WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) for data encryption.



Wireless Security

Select a Wireless Security level:

○ None ○ WEP ○ 802.1x ● WPA

Group Key Interval: 3600

Note: Group Key Interval is shared by all WPA options.

● 802.1x Server IP Address:

Port: 1812

Secret:

○ PSK String String: (Max 63 characters)

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-61 : Wireless Security - WPA

4.6.5 Wireless Management

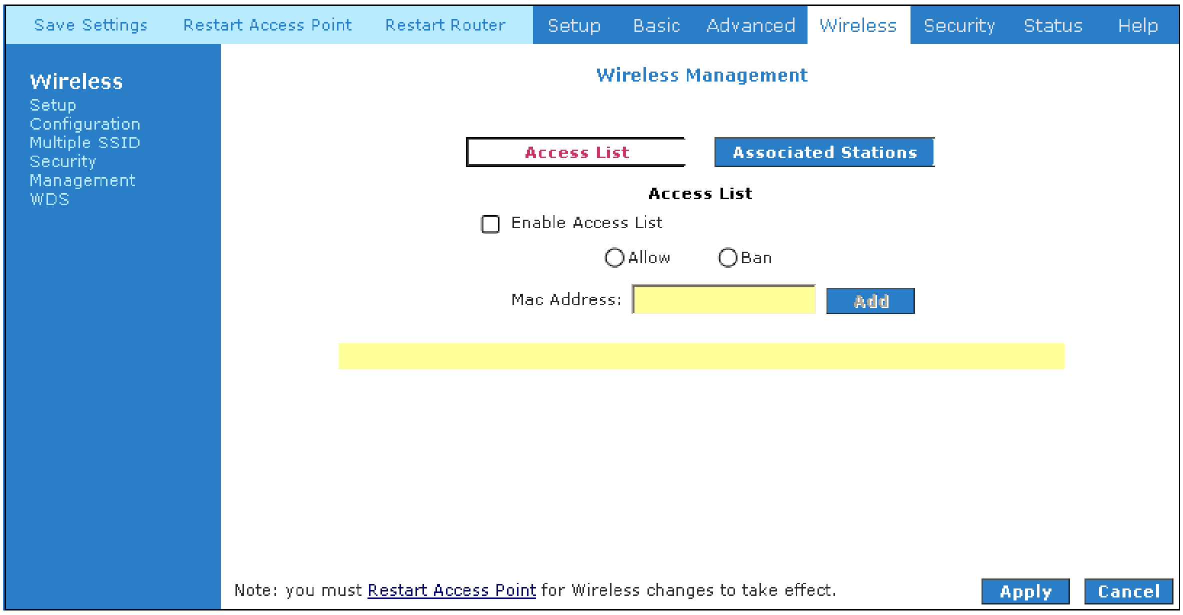
The wireless management function gives another level of security to your AP. It allows you to create an allowed access list or a banned access list (not both) and view a list of stations associated with your access point. Wireless Management consists of Access List and Associated Stations.

4.6.5.1 Access List

This feature permits you to "Allow" or "Ban" any wireless client from accessing the wireless router. You must add the MAC address of the client's wireless LAN card.

4.6.5.2 Associated Stations

Wireless client, which are connected to the wireless router, will be displayed in this screen. You are able to ban this station by clicking on the "Ban Station" option. Then click on "Apply" button.



Wireless Management

Access List

□ Enable Access List

○ Allow ○ Ban

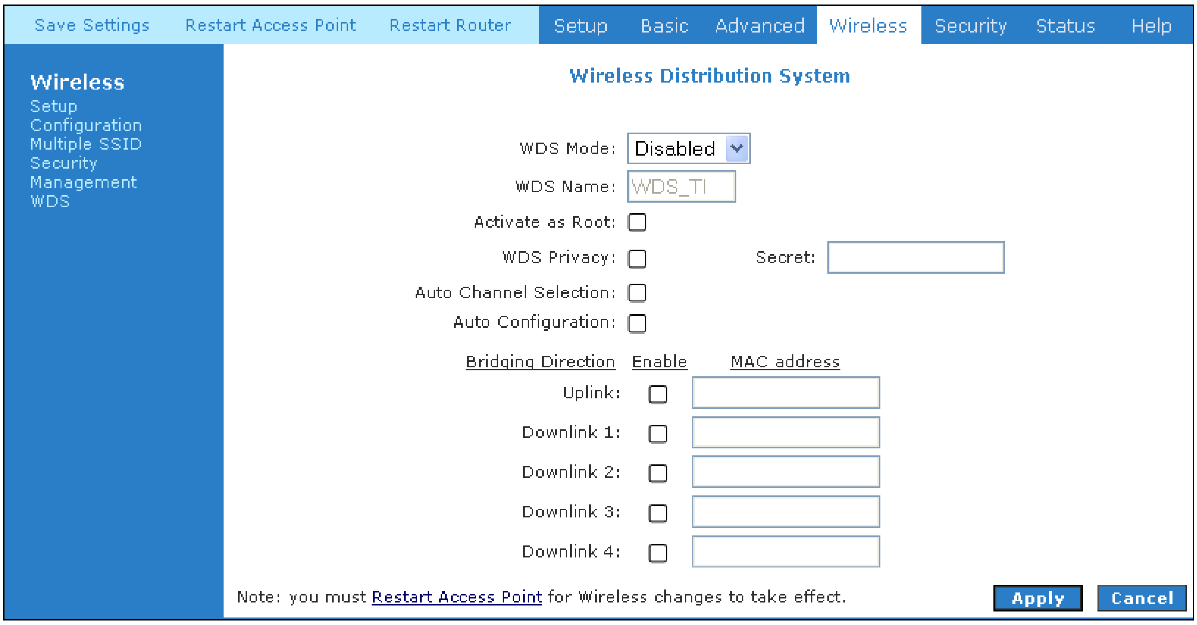
Mac Address:

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-62 : Wireless Management

4.6.6 WDS

Wireless distribution system (WDS) is a system that interconnects BSS to build a premise wide network. WDS network allows users of mobile equipment to roam and stay connected to the available network resources. You can configure your router AP as WDS mode using the WDS page.



Wireless Distribution System

WDS Mode: Disabled

WDS Name: WDS_TI

Activate as Root: □

WDS Privacy: □ Secret:

Auto Channel Selection: □

Auto Configuration: □

Bridging Direction	Enable	MAC address
Uplink:	□	
Downlink 1:	□	
Downlink 2:	□	
Downlink 3:	□	
Downlink 4:	□	

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 1-63 : WDS

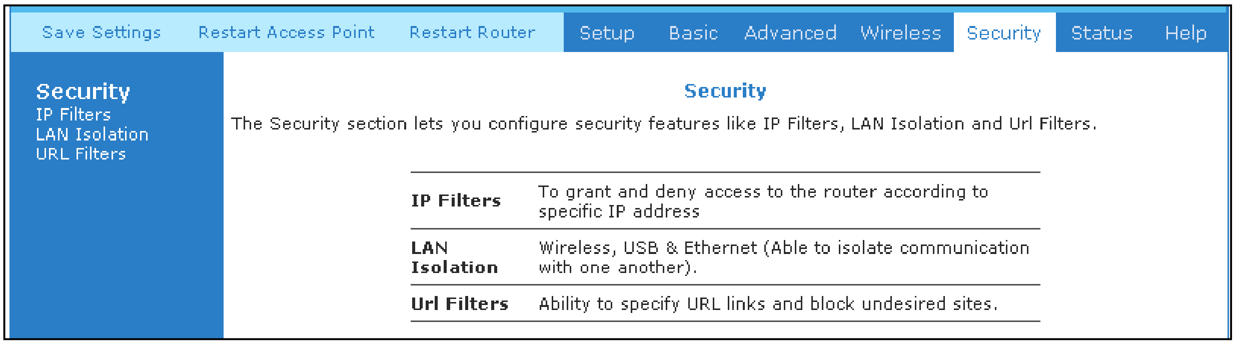
Field	**Definition/ Description**
WDS Mode	The following WDS mode are available: • Bridge: In Bridge mode, the AP basic service set (BSS) service is enabled. • Repeater: In Repeater mode, the AP BSS is disabled when connection to the upper layer AP is established. • Crude: In Crude mode, the AP BSS is always enabled; however the links between APs are configured statically and are not maintained. • Disabled (Default): WDS inactive. In both Bridge and Repeater modes, WDS uses management protocol to establish and maintain links between APs.
WDS Name	The WDS name is used to identify WDS network. The field takes up to eight characters. Two or more WDS networks may exist in the same area.

Activate as Root	This field must be checked for the root device in WDS hierarchy. Only one WDS root device may exist in WDS network. This field is not applicable for Crude mode.
WDS Privacy	Checking this field commands WDS manager to use a secured connection between APs in the WDS network. Security settings must be the same in all APs in the WDS network. Note: WDS privacy is not supported in Crude mode.
Secret	The 32-character alpha-numeric privacy key.
Auto Channel Selection	Auto channel selection is not supported in the current version.
Auto Configuration	Auto configuration is not supported in the current version.
Uplink Connection Check Box	The BSS ID of the upper device in the WDS hierarchy. This uplink cannot be configured if root is enabled.
Downlink Connection Check Boxes	The BSS ID of the lower device in the WDS hierarchy connected to this AP. Up to four downlinks can be configured.

4.7 Security

The security feature section allows users to configure the following:

- IP Filters
- LAN Isolation
- URL Filters



Security

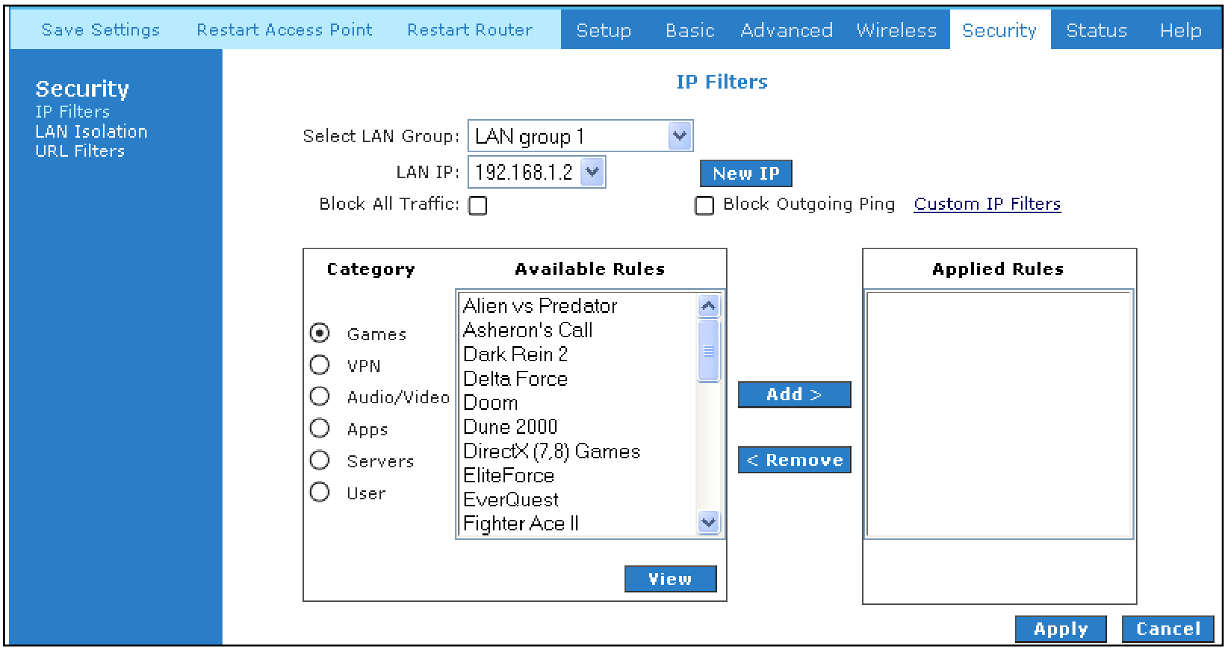
The Security section lets you configure security features like IP Filters, LAN Isolation and Url Filters.

IP Filters	To grant and deny access to the router according to specific IP address
LAN Isolation	Wireless, USB & Ethernet (Able to isolate communication with one another).
Url Filters	Ability to specify URL links and block undesired sites.

Figure 1-64 : Security

4.7.1 IP Filters

IP filter is identical to Port blocking in Access Control. The router will block workstations with defined IP range and port range. See Figure 1-65**.**



IP Filters

Select LAN Group: LAN group 1

LAN IP: 192.168.1.2

Block All Traffic: □

□ Block Outgoing Ping

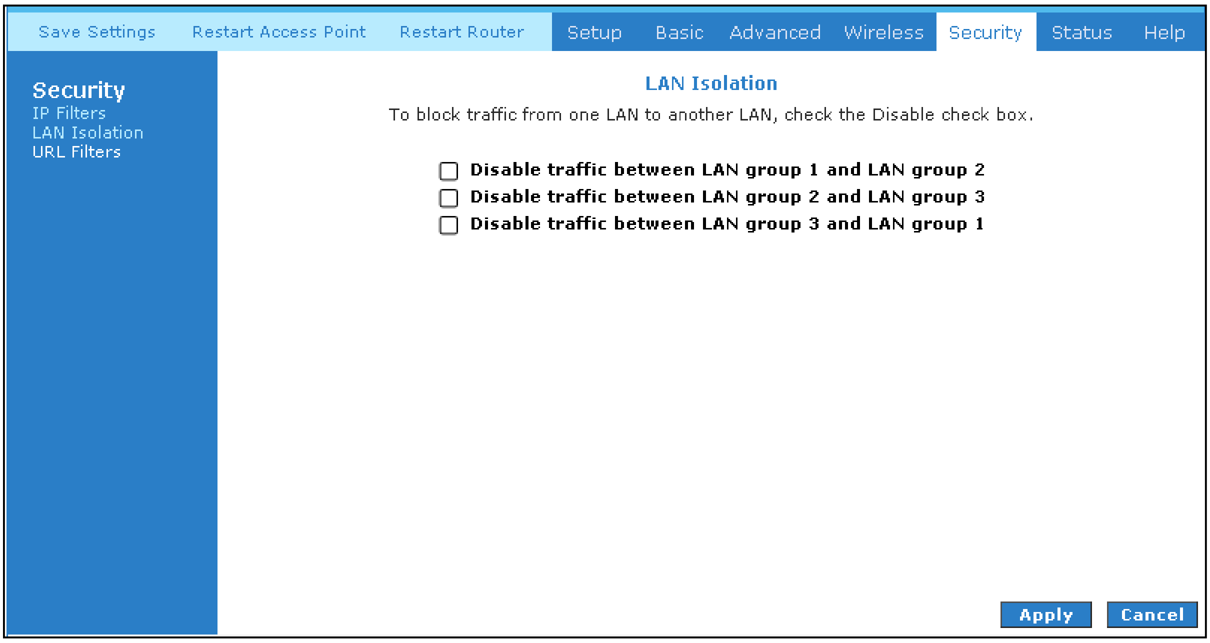
Category	Available Rules
● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User	Alien vs Predator Asheron's Call Dark Rein 2 Delta Force Doom Dune 2000 DirectX (7,8) Games EliteForce EverQuest Fighter Ace II

Applied Rules

Figure 1-65 : IP Filters

4.7.2 LAN Isolation

LAN isolation allows you to disable the flow of packets up to three user-defined LAN groups (WLAN, USB, and Ethernet). This allows you to secure information in private portions of the LAN from other publicly accessible LAN segments.



LAN Isolation

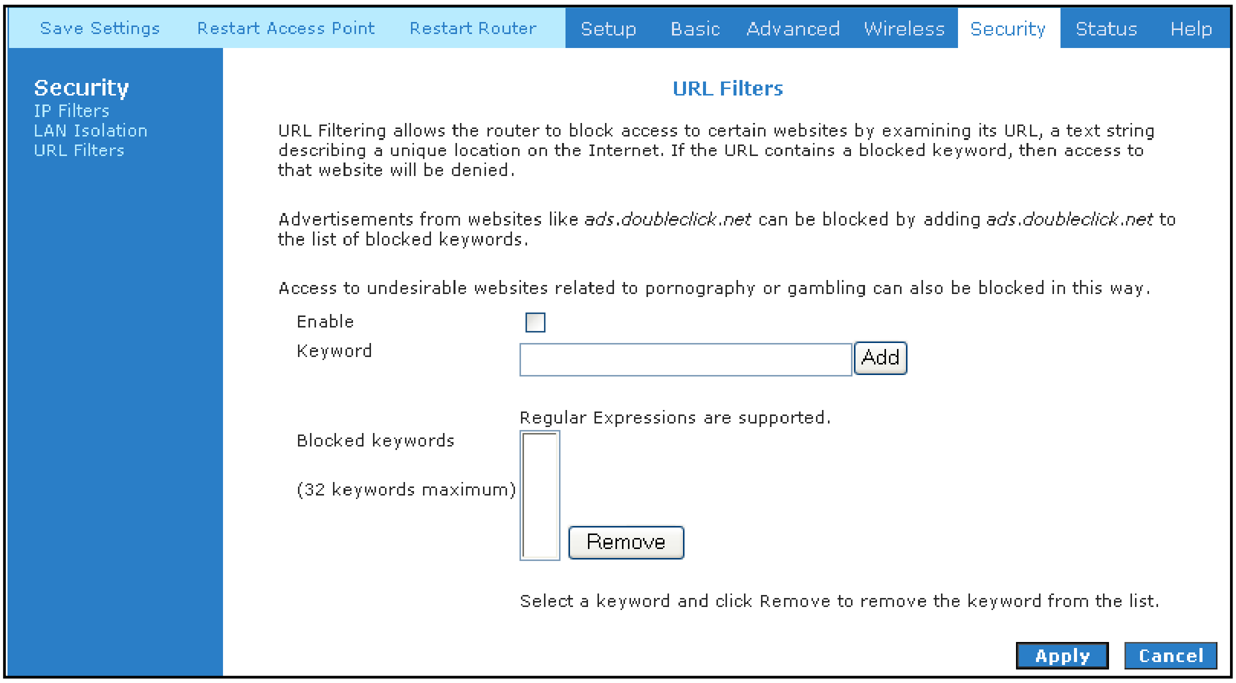
To block traffic from one LAN to another LAN, check the Disable check box.

□ Disable traffic between LAN group 1 and LAN group 2
□ Disable traffic between LAN group 2 and LAN group 3
□ Disable traffic between LAN group 3 and LAN group 1

Figure 1-66 : LAN Isolation

4.7.3 URL Filters

This feature allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied. See Figure 1-67**.**



URL Filters

URL Filtering allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied.

Advertisements from websites like *ads.doubleclick.net* can be blocked by adding *ads.doubleclick.net* to the list of blocked keywords.

Access to undesirable websites related to pornography or gambling can also be blocked in this way.

Enable □

Keyword

Regular Expressions are supported.

Blocked keywords

(32 keywords maximum)

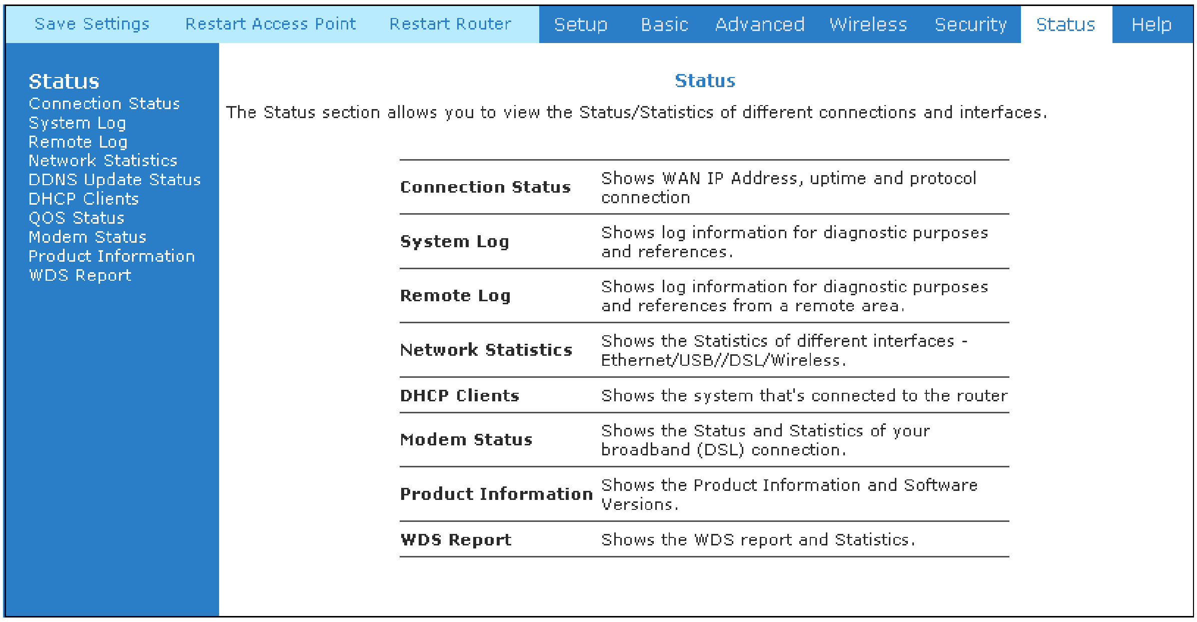
Select a keyword and click Remove to remove the keyword from the list.

Figure 1-67 : URL Filters

4.8 Status

This status section allows users to view the following connections and interfaces:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DDNS Update Status
- DHCP Clients
- QoS Status
- Modem Status
- Product Information
- WDS Report



Status

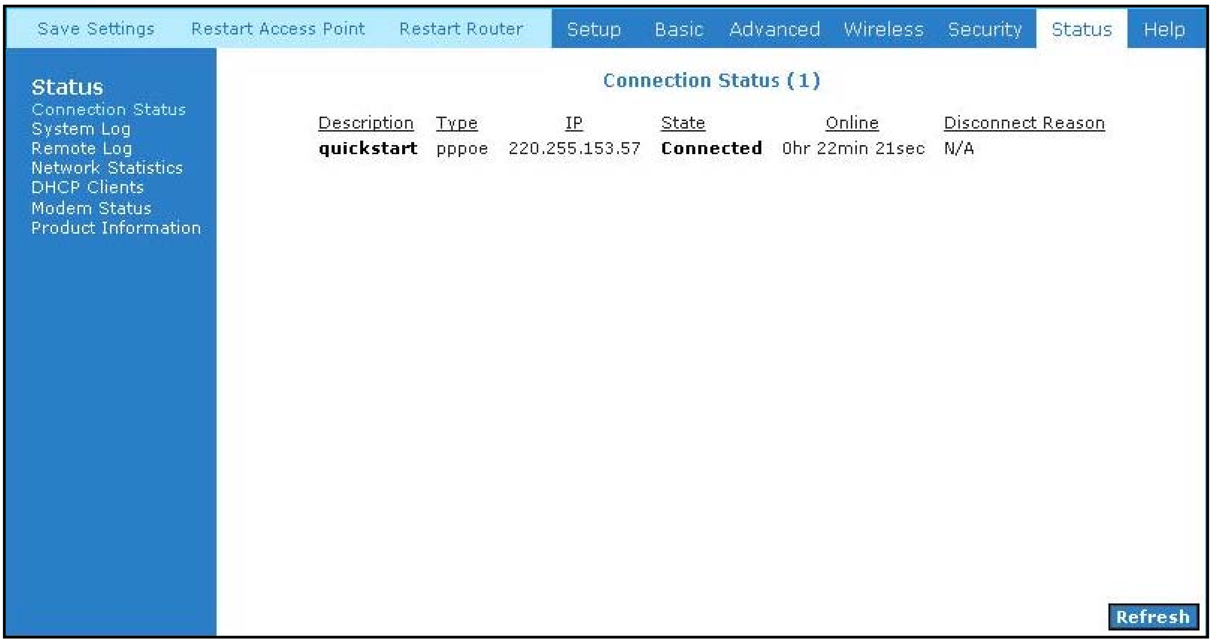
The Status section allows you to view the Status/Statistics of different connections and interfaces.

Connection Status	Shows WAN IP Address, uptime and protocol connection
System Log	Shows log information for diagnostic purposes and references.
Remote Log	Shows log information for diagnostic purposes and references from a remote area.
Network Statistics	Shows the Statistics of different interfaces - Ethernet/USB//DSL/Wireless.
DHCP Clients	Shows the system that's connected to the router
Modem Status	Shows the Status and Statistics of your broadband (DSL) connection.
Product Information	Shows the Product Information and Software Versions.
WDS Report	Shows the WDS report and Statistics.

Figure 1-68 : Status

4.8.1 Connection Status

Connection Status will display all the relevant information regarding your Internet Connection. It will display the type of protocol used, the WAN IP address, the connection state and the duration connected. See Figure 1-69.



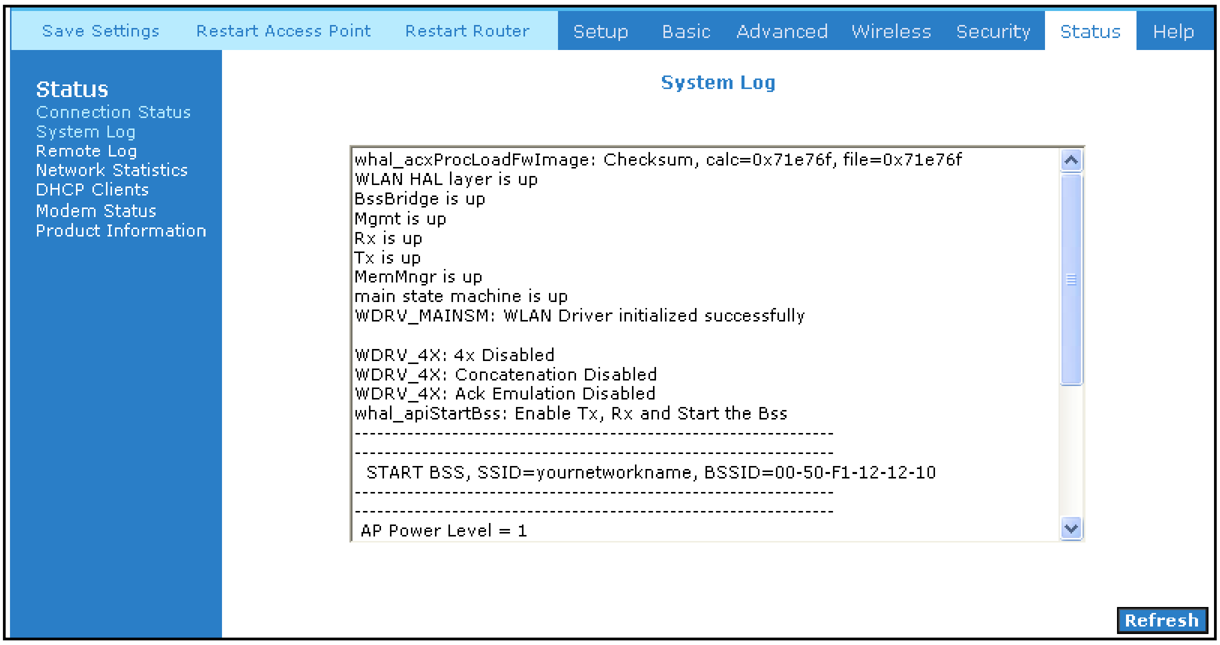
Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	220.255.153.57	**Connected**	0hr 22min 21sec	N/A

Figure 1-69 : Connection Status

4.8.2 System Log

You can view the ADSL Router's logged information. Depending upon the severity level, this logged information will generate log reports to a remote host (if remote logging is enabled). See Figure 1-70.



System Log

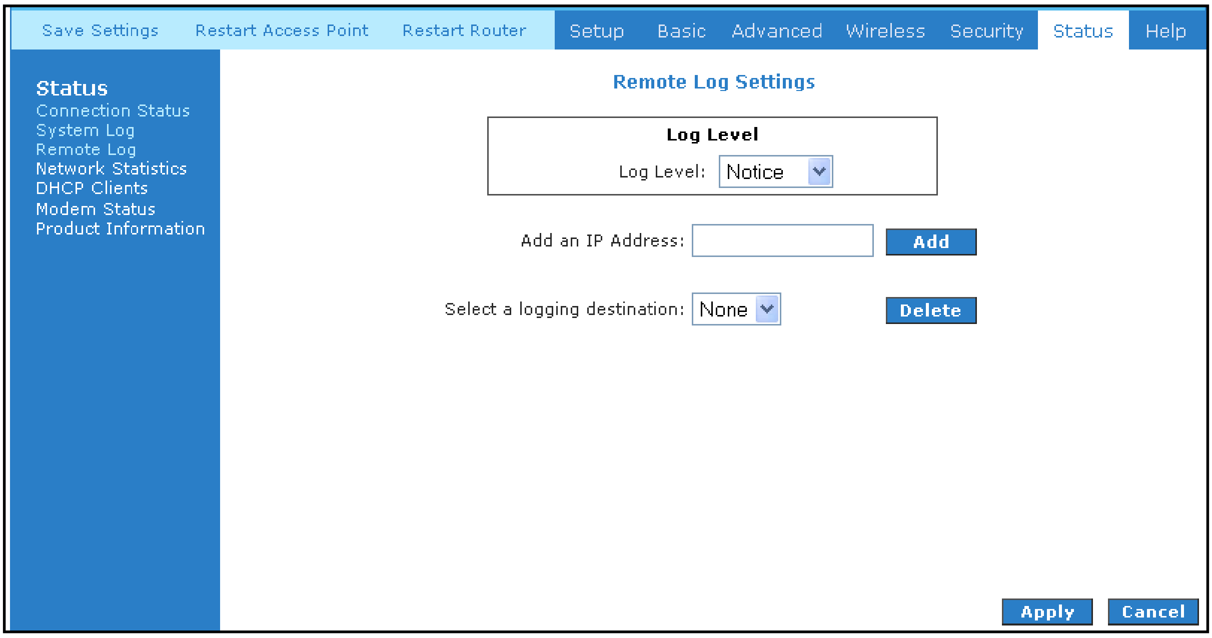
```
whal_acxProcLoadFwImage: Checksum, calc=0x71e76f, file=0x71e76f
WLAN HAL layer is up
BssBridge is up
Mgmt is up
Rx is up
Tx is up
MemMngr is up
main state machine is up
WDRV_MAINSM: WLAN Driver initialized successfully

WDRV_4X: 4x Disabled
WDRV_4X: Concatenation Disabled
WDRV_4X: Ack Emulation Disabled
whal_apiStartBss: Enable Tx, Rx and Start the Bss
------------------------------------------------------------
------------------------------------------------------------
 START BSS, SSID=yournetworkname, BSSID=00-50-F1-12-12-10
------------------------------------------------------------
------------------------------------------------------------
 AP Power Level = 1
```

Figure 1-70 : System Log

4.8.3 Remote Log Settings

This feature is for users to enable remote logging. Settings mentioned below are essential for this feature to work. See Figure 1-71**.**

- Log Level
- Adding / Deleting IP address
- Logging destination



Remote Log Settings

Log Level

Log Level: Notice

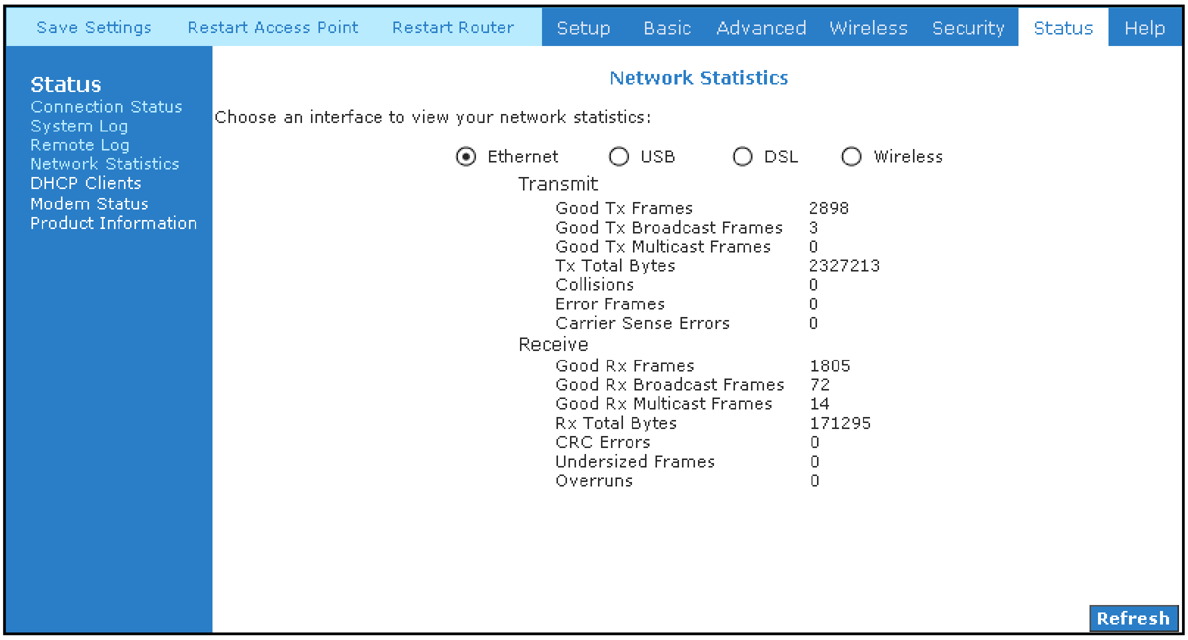
Add an IP Address:

Select a logging destination: None

Figure 1-71 : Remote Log Settings

4.8.4 Network Statistics

Information regarding the Status and Statistics of your Ethernet, USB, DSL and Wireless line will be displayed.



Network Statistics

Choose an interface to view your network statistics:

● Ethernet ○ USB ○ DSL ○ Wireless

Transmit

Good Tx Frames	2898
Good Tx Broadcast Frames	3
Good Tx Multicast Frames	0
Tx Total Bytes	2327213
Collisions	0
Error Frames	0
Carrier Sense Errors	0

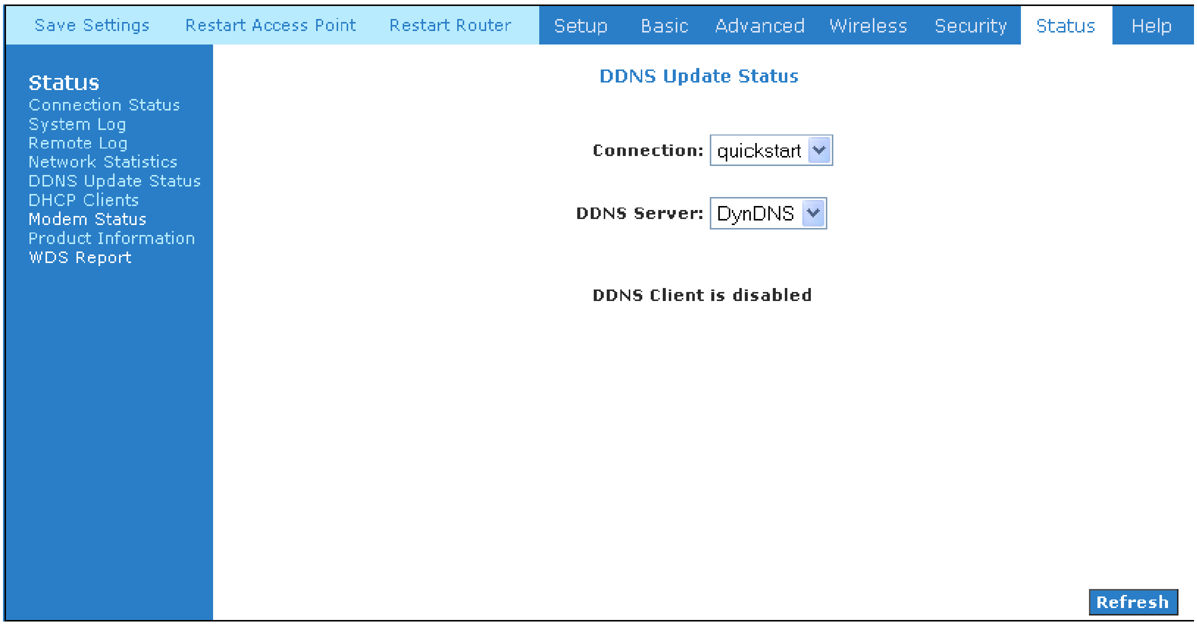
Receive

Good Rx Frames	1805
Good Rx Broadcast Frames	72
Good Rx Multicast Frames	14
Rx Total Bytes	171295
CRC Errors	0
Undersized Frames	0
Overruns	0

Figure 1-72 : Network Statistics

4.8.5 DDNS Update Status

You can view the DDNS update status of your WAN connection from the **DDNS Status** page. See Figure 1-73. To access, click the **DDNS Update Status** link from the **Status** main page.



DDNS Update Status

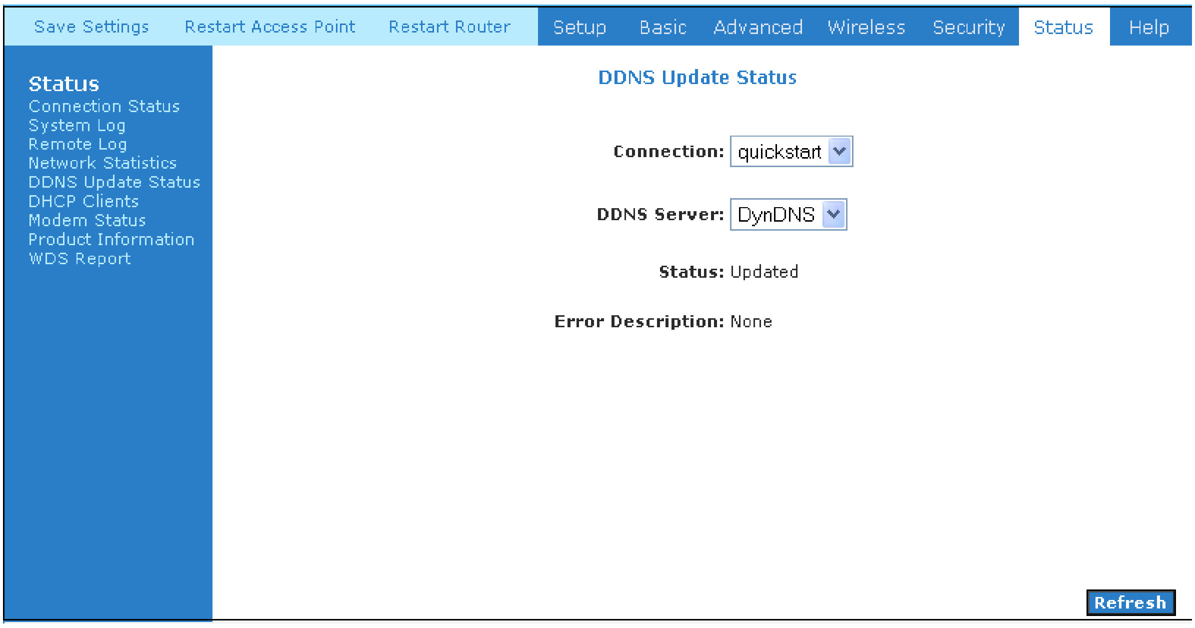
Connection: quickstart

DDNS Server: DynDNS

DDNS Client is disabled

Figure 1-73 : DDNS Update Status

As you can see from this page, the DDNS client is disabled by default for your router. To enable the DDNS client feature, refer to Chapter 4.5.18. When DDNS client is enabled, the DDNS client updates every time the router gets a new IP address. The DDNS Status page (Figure 1-74) provides you the DDNS update status of your router.



DDNS Update Status

Connection: quickstart

DDNS Server: DynDNS

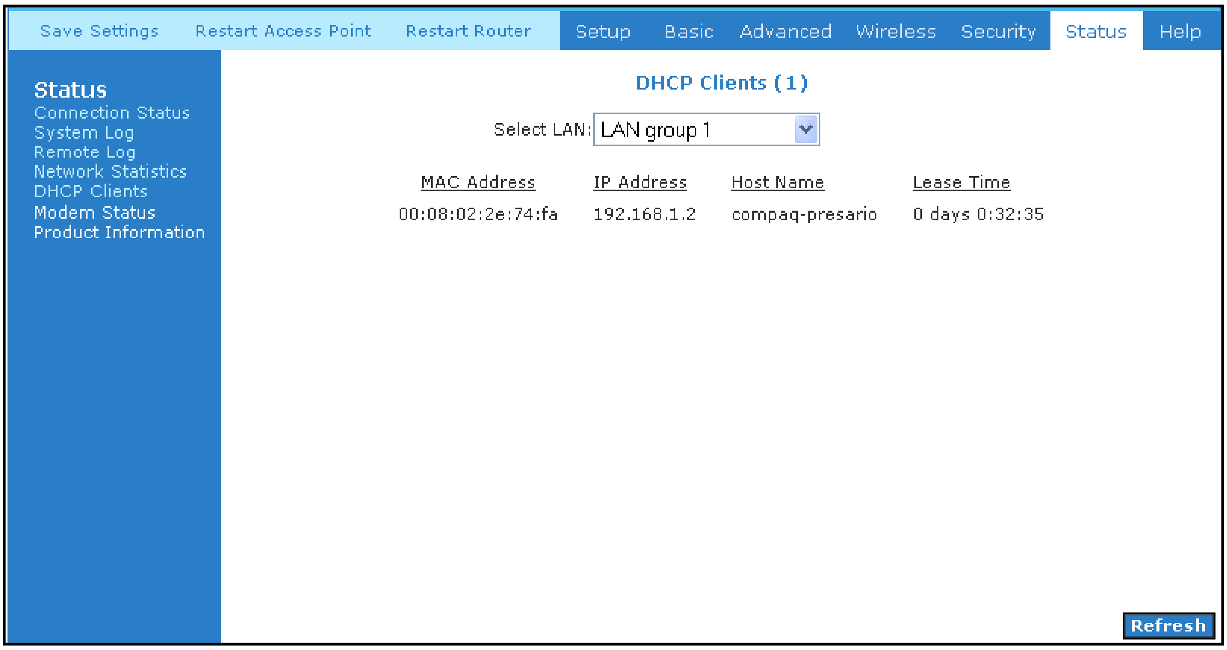
Status: Updated

Error Description: None

Figure 1-74 : DDNS Status (DDNS Client Enabled)

4.8.6 DHCP Clients

This section shows the users connected. It also shows the MAC address, IP address, host name and lease time.



DHCP Clients (1)

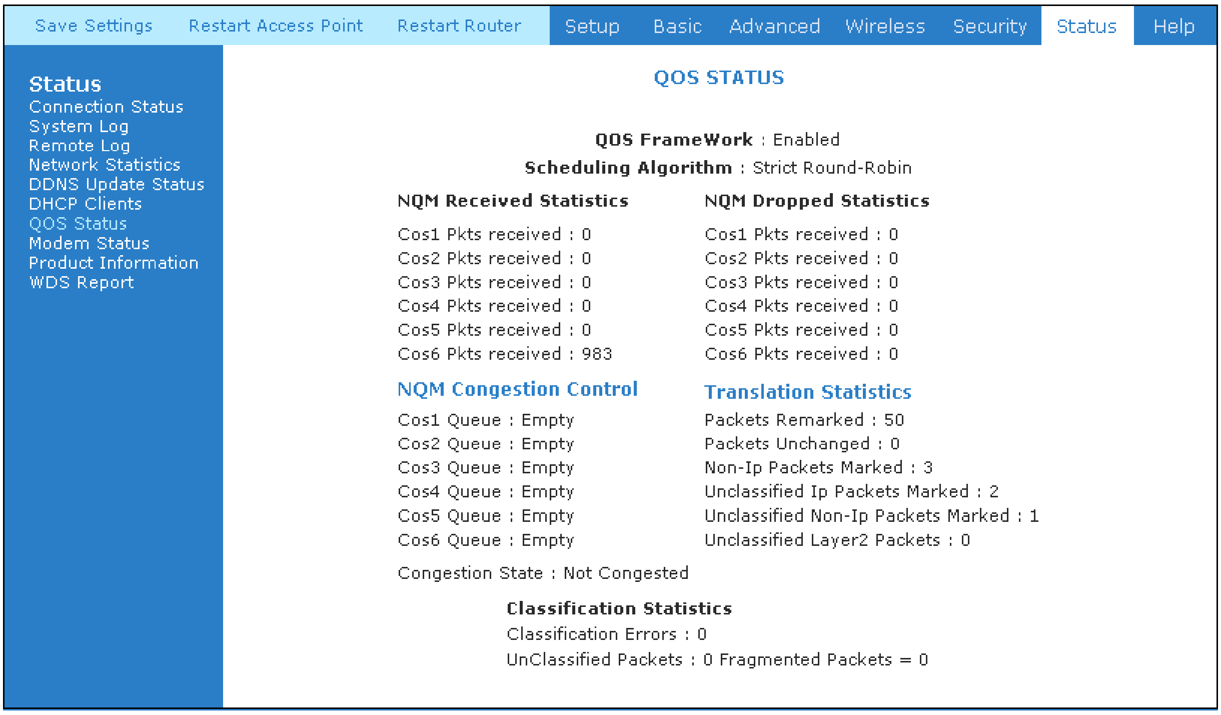
Select LAN: LAN group 1

MAC Address	IP Address	Host Name	Lease Time
00:08:02:2e:74:fa	192.168.1.2	compaq-presario	0 days 0:32:35

Figure 1-75 : DHCP Clients

4.8.7 QoS Status

This section displays the QoS status and shows which packets have been received or dropped.



QOS STATUS

QOS FrameWork : Enabled

Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics

Cos1 Pkts received : 0
Cos2 Pkts received : 0
Cos3 Pkts received : 0
Cos4 Pkts received : 0
Cos5 Pkts received : 0
Cos6 Pkts received : 983

NQM Dropped Statistics

Cos1 Pkts received : 0
Cos2 Pkts received : 0
Cos3 Pkts received : 0
Cos4 Pkts received : 0
Cos5 Pkts received : 0
Cos6 Pkts received : 0

NQM Congestion Control

Cos1 Queue : Empty
Cos2 Queue : Empty
Cos3 Queue : Empty
Cos4 Queue : Empty
Cos5 Queue : Empty
Cos6 Queue : Empty

Congestion State : Not Congested

Translation Statistics

Packets Remarked : 50
Packets Unchanged : 0
Non-Ip Packets Marked : 3
Unclassified Ip Packets Marked : 2
Unclassified Non-Ip Packets Marked : 1
Unclassified Layer2 Packets : 0

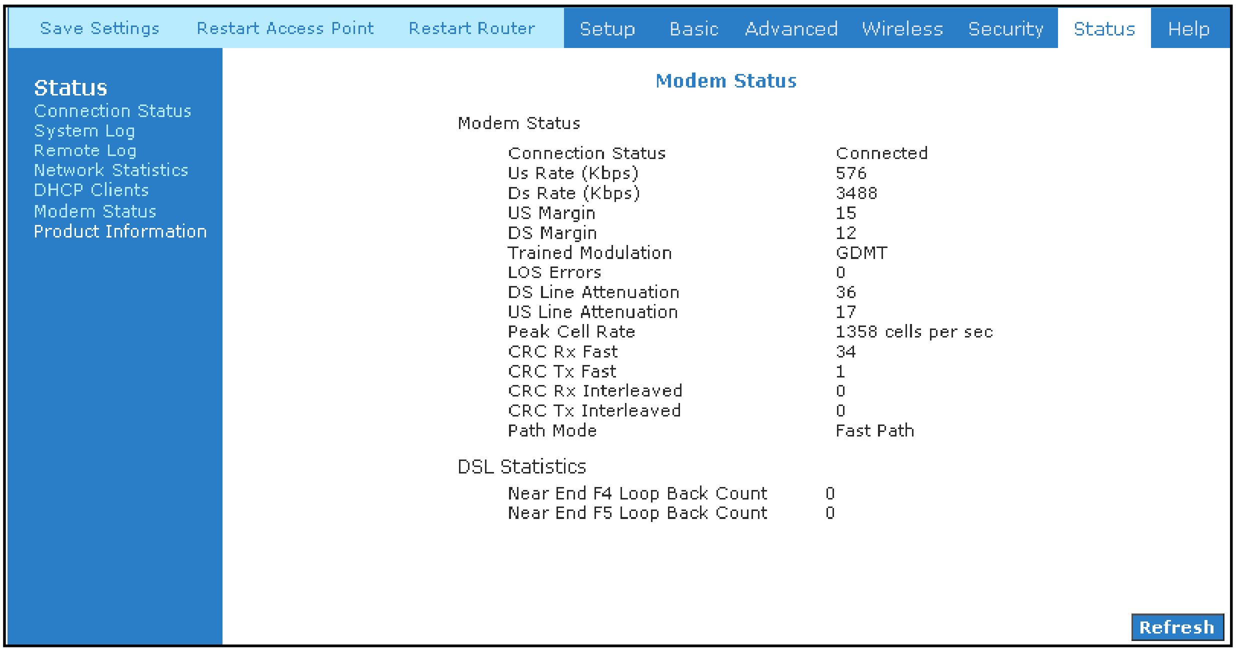
Classification Statistics

Classification Errors : 0
UnClassified Packets : 0 Fragmented Packets = 0

Figure 1-76 : QoS Status

4.8.8 Modem Status

This section displays the Modem status and DSL statistics.



Modem Status

Modem Status

Connection Status	Connected
Us Rate (Kbps)	576
Ds Rate (Kbps)	3488
US Margin	15
DS Margin	12
Trained Modulation	GDMT
LOS Errors	0
DS Line Attenuation	36
US Line Attenuation	17
Peak Cell Rate	1358 cells per sec
CRC Rx Fast	34
CRC Tx Fast	1
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path

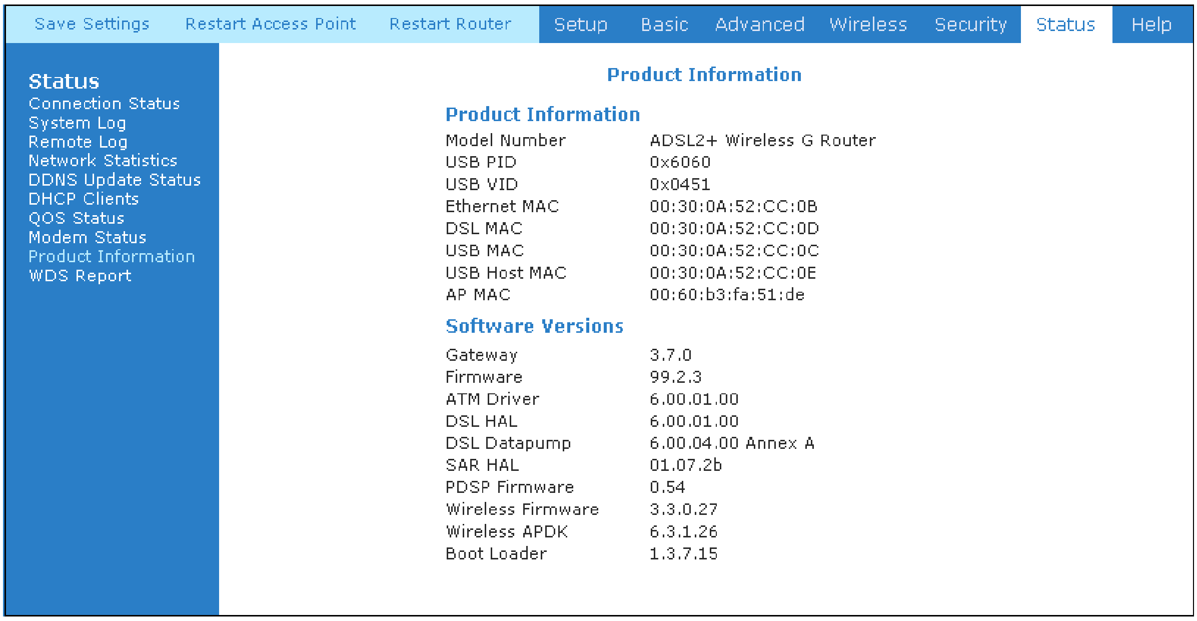
DSL Statistics

Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

Figure 1-77 : Modem Status

4.8.9 Product Information

This screen shows a summary of all the product information and software version that comes bundled with the ADSL Router. You can display the information by clicking the **Product Information** link on the **Status** main page as shown in Figure 1-78.



Product Information

Product Information

Model Number	ADSL2+ Wireless G Router
USB PID	0x6060
USB VID	0x0451
Ethernet MAC	00:30:0A:52:CC:0B
DSL MAC	00:30:0A:52:CC:0D
USB MAC	00:30:0A:52:CC:0C
USB Host MAC	00:30:0A:52:CC:0E
AP MAC	00:60:b3:fa:51:de

Software Versions

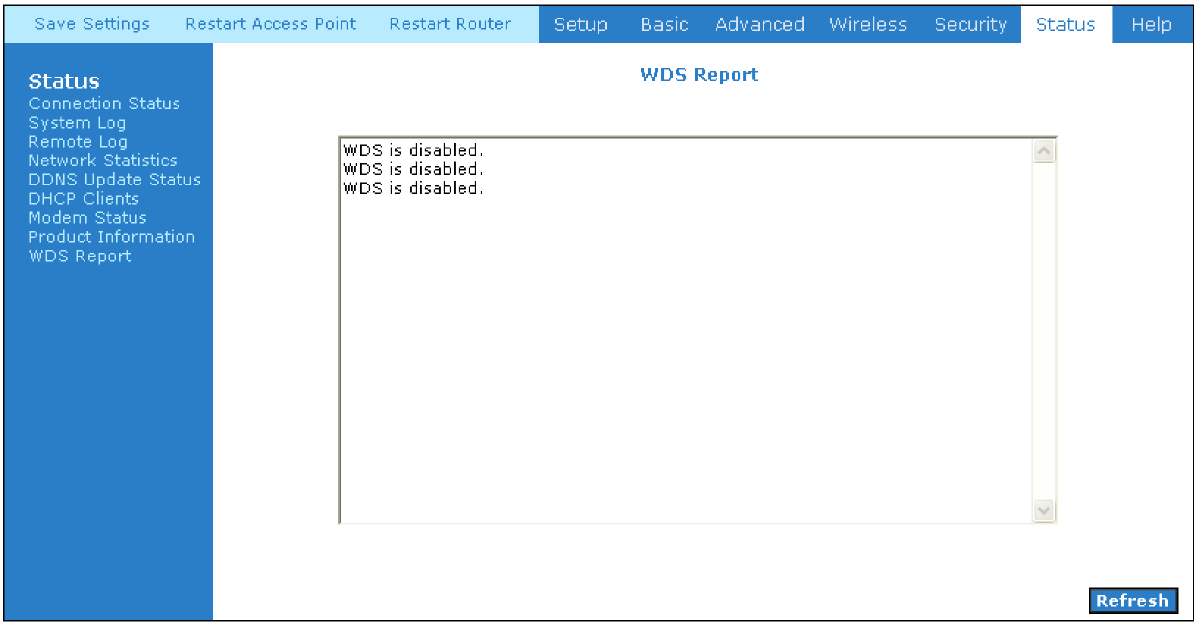
Gateway	3.7.0
Firmware	99.2.3
ATM Driver	6.00.01.00
DSL HAL	6.00.01.00
DSL Datapump	6.00.04.00 Annex A
SAR HAL	01.07.2b
PDSP Firmware	0.54
Wireless Firmware	3.3.0.27
Wireless APDK	6.3.1.26
Boot Loader	1.3.7.15

Figure 1-78 : Product Information

4.8.10 WDS Report

You can view the WDS report for your router (AP) by clicking the WDS Report link from the Status main page. The WDS Report page (Figure 1-79) allows you to view the following WDS-related wireless activities:

- WDS configuration and states
- WDS management statistics
- WDS database

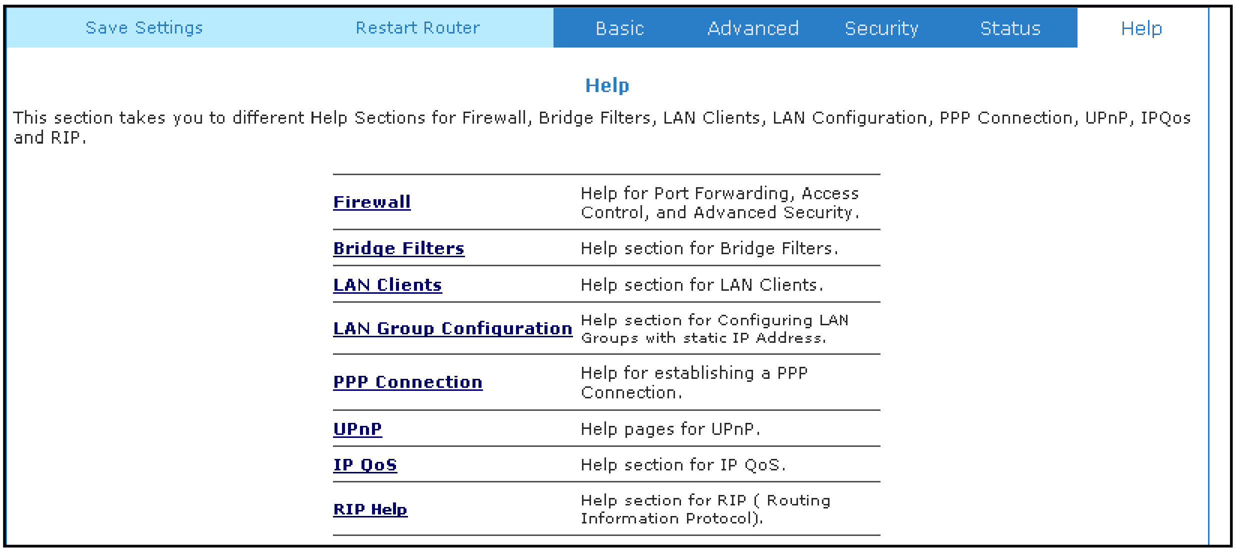


```
WDS is disabled.
WDS is disabled.
WDS is disabled.
```

Figure 1-79 : WDS Report

4.9 Help

The Help screen takes you to the different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Group Configurations, PPP Connection, UPnP, IP QoS and RIP Help.



Help

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Configuration, PPP Connection, UPnP, IPQos and RIP.

Firewall	Help for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
LAN Group Configuration	Help section for Configuring LAN Groups with static IP Address.
PPP Connection	Help for establishing a PPP Connection.
UPnP	Help pages for UPnP.
IP QoS	Help section for IP QoS.
RIP Help	Help section for RIP (Routing Information Protocol).

Figure 1-80 : Help Screen